PCT/JP01/00772

02.02.01

JP04/7?2

EU

9/8 #4

日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２０００年１２月１３日

出願番号
Application Number: 特願２０００－３７９３６１

出願人
Applicant (s): ソニー株式会社

09/937797

PRIORITY DOCUMENT

SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

２００１年　３月　２日

特許庁長官
Commissioner,
Patent Office 及川耕造

出証番号　出証特２００１

【書類名】　特許願

【整理番号】　0000895928

【提出日】　平成12年12月13日

【あて先】　特許庁長官殿

【国際特許分類】　G06F 17/60

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　金巻　裕史

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　佐竹　清

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　齋藤　真

【発明者】

【住所又は居所】　東京都中央区日本橋室町１丁目６番地３号　ソニーケミカル株式会社内

【氏名】　中村　嘉秀

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　橋本　主税

【特許出願人】

【識別番号】　000002185

【氏名又は名称】　ソニー株式会社

【代表者】　出井　伸之

【代理人】

【識別番号】　100094053

【弁理士】

【氏名又は名称】　佐藤　隆久

【先の出願に基づく優先権主張】

【出願番号】　特願2000- 24619

【出願日】　平成12年 2月 2日

【先の出願に基づく優先権主張】

【出願番号】　特願2000-209674

【出願日】　平成12年 7月11日

【先の出願に基づく優先権主張】

【出願番号】　特願2000-209675

【出願日】　平成12年 7月11日

【先の出願に基づく優先権主張】

【出願番号】　特願2000-234741

【出願日】　平成12年 8月 2日

【先の出願に基づく優先権主張】

【出願番号】　特願2000-234752

【出願日】　平成12年 8月 2日

【先の出願に基づく優先権主張】

【出願番号】　特願2000-238077

【出願日】　平成12年 8月 7日

【先の出願に基づく優先権主張】

【出願番号】　特願2000-370519

【出願日】　平成12年12月 5日

【手数料の表示】

【予納台帳番号】　014890

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9707389

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　認証装置、認証システムおよびその方法、処理装置、通信装置、通信制御装置、通信システムおよびその方法、情報記録方法およびその装置、情報復元方法およびその装置、その記録媒体

【特許請求の範囲】

【請求項１】

ネットワークを介して少なくとも２者間で行われる取り引きを認証する認証装置において、

第１の取り引き者の個人識別情報、第２の取り引き者の個人識別情報および取り引き内容を示す情報を含む第１の要求を、前記第１の取り引き者から受信する第１の受信手段と、

前記第１の要求に応じて、前記第１の取り引き者の正当性を認証して第１の認証情報を生成する第１の認証手段と、

前記第１の認証情報および前記取り引きの内容を示す情報を含む第２の要求を前記第２の取り引き者に送信する第１の送信手段と、

前記第２の要求に対しての応答を前記第２の取り引き者から受信する第２の受信手段と、

前記応答に応じて、前記第２の取り引き者の正当性を認証して第２の認証情報を生成する第２の認証手段と、

前記第２の認証情報を前記第１の取り引き者に送信する第２の送信手段と

を有する認証装置。

【請求項２】

前記第１の受信手段は、前記第１の取り引き者の個人キー情報をさらに含む前記第１の要求を受信し、

前記第１の認証手段は、前記個人キー情報に基づいて前記第１の取り引き者の正当性を認証し、

前記第２の受信手段は、前記第２の取り引き者の個人キー情報を含む前記応答を受信し、

前記第１の認証手段は、前記第２の取り引き者の個人キー情報に基づいて前記

第２の取り引き者の正当性を認証する

請求項１に記載の認証装置。

【請求項３】

前記第１の取り引き者および前記第２の取り引き者の前記個人キー情報は、それぞれ前記第１の取り引き者および前記第２の取り引き者の課金に係わる情報である

請求項２に記載の認証装置。

【請求項４】

前記第１の送信手段は、前記第１の取り引き者の前記個人キー情報をさらに含む第２の要求を前記第２の取り引き者に送信する

請求項３に記載の認証装置。

【請求項５】

前記取り引きの履歴を示す履歴情報を記憶する記憶手段

をさらに有する請求項１に記載の認証装置。

【請求項６】

前記第１の要求が暗号化されている場合に、前記受信した第１の要求を復号する復号手段

をさらに有する請求項１に記載の認証装置。

【請求項７】

前記第２の要求を暗号化する暗号化手段

をさらに有する請求項１に記載の認証装置。

【請求項８】

前記応答が暗号化されている場合に、前記受信した応答を復号する復号手段

をさらに有する請求項１に記載の認証装置。

【請求項９】

前記第２の認証情報を暗号化する暗号化手段

をさらに有する請求項１に記載の認証装置。

【請求項１０】

ネットワークを介して少なくとも２者間で行われる取り引きを認証する認証シ

ステムにおいて、

第１の取り引き者が使用する第１の通信装置と、

第２の取り引き者が使用する第２の通信装置と、

前記取り引きを認証する認証装置と

を有し、

前記第１の通信装置は、第１の取り引き者の個人識別情報、第２の取り引き者の個人識別情報および取り引き内容を示す情報を含む第１の要求を前記認証装置に送信し、

前記認証装置は、

前記第１の取り引き者から前記第１の要求を受信する第１の受信手段と、

前記第１の要求に応じて、前記第１の取り引き者の正当性を認証して第１の認証情報を生成する第１の認証手段と、

前記第１の認証情報および前記取り引きの内容を示す情報を含む第２の要求を前記第２の取り引き者に送信する第１の送信手段と、

前記第２の要求に対しての応答を前記第２の取り引き者から受信する第２の受信手段と、

前記応答に応じて、前記第２の取り引き者の正当性を認証して第２の認証情報を生成する第２の認証手段と、

前記第２の認証情報を前記第１の取り引き者に送信する第２の送信手段と

を有する

認証システム。

【請求項１１】

前記第１の受信手段は、前記第１の取り引き者の個人キー情報をさらに含む前記第１の要求を受信し、

前記第１の認証手段は、前記個人キー情報に基づいて前記第１の取り引き者の正当性を認証し、

前記第２の受信手段は、前記第２の取り引き者の個人キー情報を含む前記応答を受信し、

前記第１の認証手段は、前記第２の取り引き者の個人キー情報に基づいて前記

第２の取り引き者の正当性を認証する

請求項１０に記載の認証システム。

【請求項１２】

前記第１の取り引き者および前記第２の取り引き者の前記個人キー情報は、それぞれ前記第１の取り引き者および前記第２の取り引き者の課金に係わる情報である

請求項１１に記載の認証システム。

【請求項１３】

ネットワークを介して少なくとも２者間で行われる取り引きを認証する認証方法において、

第１の取り引き者の個人識別情報、第２の取り引き者の個人識別情報および取り引き内容を示す情報を含む第１の要求を、前記第１の取り引き者から受信し、

前記第１の要求に応じて、前記第１の取り引き者の正当性を認証して第１の認証情報を生成し、

前記第１の認証情報および前記取り引きの内容を示す情報を含む第２の要求を前記第２の取り引き者に送信し、

前記第２の要求に対しての応答を前記第２の取り引き者から受信し、

前記応答に応じて、前記第２の取り引き者の正当性を認証して第２の認証情報を生成し、

前記第２の認証情報を前記第１の取り引き者に送信する

認証方法。

【請求項１４】

前記第１の取り引き者の個人キー情報をさらに含む前記第１の要求を受信し、

前記個人キー情報に基づいて前記第１の取り引き者の正当性を認証し、

前記第２の取り引き者の個人キー情報を含む前記応答を受信し、

前記第２の取り引き者の個人キー情報に基づいて前記第２の取り引き者の正当性を認証する

請求項１３に記載の認証方法。

【請求項１５】

前記第１の取り引き者および前記第２の取り引き者の前記個人キー情報は、それぞれ前記第１の取り引き者および前記第２の取り引き者の課金に係わる情報である

請求項１４に記載の認証方法。

【請求項１６】

前記第１の取り引き者の前記個人キー情報をさらに含む第２の要求を前記第２の取り引き者に送信する

請求項１５に記載の認証方法。

【請求項１７】

前記第２の取り引き者は、前記第１の取り引き者の個人キー情報を用いて決済を行う

請求項１６に記載の認証方法。

【請求項１８】

ネットワークを介して少なくとも２者間で行われる取り引きを認証する認証装置において、

第１の取り引き者の個人識別情報、前記第１の取り引き者の個人キー情報、第２の取り引き者の個人識別情報および取り引き内容を示す情報を含む第１の要求を、前記第１の取り引き者から受信する第１の受信手段と、

前記第１の要求に含まれる前記個人キー情報に基づいて前記第１の取り引き者の正当性を認証して第１の認証情報を生成する第１の認証手段と、

前記第１の要求から前記第１の取り引き者の個人キー情報を除去した情報と、前記第１の認証情報とを含む第２の要求を前記第２の取り引き者に送信する第１の送信手段と、

前記第２の要求に対しての応答を前記第２の取り引き者から受信する第２の受信手段と、

前記応答に応じて、前記第２の取り引き者の正当性を認証して第２の認証情報を生成する第２の認証手段と、

前記第２の認証情報を前記第１の取り引き者に送信する第２の送信手段と

を有する認証装置。

【請求項１９】

前記第２の受信手段は、前記第２の取り引き者の個人キー情報を含む前記応答を受信し、

前記第１の認証手段は、前記第２の取り引き者の個人キー情報に基づいて前記第２の取り引き者の正当性を認証する

請求項１８に記載の認証装置。

【請求項２０】

前記第１の取り引き者の個人キー情報は前記第１の取り引き者の課金に係わる情報であり、前記第２の取り引き者の個人キー情報は前記第２の取り引き者の課金に係わる情報である

請求項１９に記載の認証装置。

【請求項２１】

前記取り引きの履歴を示す履歴情報を記憶する記憶手段

をさらに有する請求項１８に記載の認証装置。

【請求項２２】

ネットワークを介して少なくとも２者間で行われる取り引きを認証する認証システムにおいて、

第１の取り引き者が使用する第１の通信装置と、

第２の取り引き者が使用する第２の通信装置と、

前記取り引きを認証する認証装置と

を有し、

前記認証装置は、

第１の取り引き者の個人識別情報、前記第１の取り引き者の個人キー情報、第２の取り引き者の個人識別情報および取り引き内容を示す情報を含む第１の要求を、前記第１の取り引き者から受信する第１の受信手段と、

前記第１の要求に含まれる前記個人キー情報に基づいて前記第１の取り引き者の正当性を認証して第１の認証情報を生成する第１の認証手段と、

前記第１の要求から前記第１の取り引き者の個人キー情報を除去した情報と、前記第１の認証情報とを含む第２の要求を前記第２の取り引き者に送信する第１

の送信手段と、

前記第２の要求に対しての応答を前記第２の取り引き者から受信する第２の受信手段と、

前記応答に応じて、前記第２の取り引き者の正当性を認証して第２の認証情報を生成する第２の認証手段と、

前記第２の認証情報を前記第１の取り引き者に送信する第２の送信手段と

を有する

認証システム。

【請求項２３】

ネットワークを介して少なくとも２者間で行われる取り引きを認証する認証方法において、

第１の取り引き者の個人識別情報、前記第１の取り引き者の個人キー情報、第２の取り引き者の個人識別情報および取り引き内容を示す情報を含む第１の要求を、前記第１の取り引き者から受信し、

前記第１の要求に含まれる前記個人キー情報に基づいて前記第１の取り引き者の正当性を認証して第１の認証情報を生成し、

前記第１の要求から前記第１の取り引き者の個人キー情報を除去した情報と、前記第１の認証情報とを含む第２の要求を前記第２の取り引き者に送信し、

前記第２の要求に対しての応答を前記第２の取り引き者から受信し、

前記応答に応じて、前記第２の取り引き者の正当性を認証して第２の認証情報を生成し、

前記第２の認証情報を前記第１の取り引き者に送信する

認証方法。

【請求項２４】

前記第１の取り引き者の個人キー情報を用いて、前記取り引きの決済を行う

請求項２３に記載の認証方法。

【請求項２５】

認証要求に応じて認証処理を行う認証装置であって、

利用者を識別するための個人識別情報と、前記認証要求の送信元の装置を識別

する装置識別情報とを含む前記認証要求を受信する受信手段と、

前記個人識別情報と認証結果を送信する送信先の情報とを対応付けて記憶する記憶手段と、

前記認証要求に応じて認証処理を行う認証処理手段と、

前記認証要求に含まれる前記個人識別情報に対応する前記送信先の情報を前記記憶手段から読み出し、当該読み出した前記送信先の情報によって特定された送信先に、前記認証処理の結果と前記認証要求に含まれる前記装置識別情報とを対応付けて送信する送信手段と

を有する認証装置。

【請求項２６】

前記受信手段は、暗号化された前記個人識別情報および前記装置識別情報を含む前記認証要求を受信し、

前記認証装置は、

前記受信した認証要求に含まれる前記個人識別情報および前記装置識別情報を復号する復号手段

をさらに有する請求項２５に記載の認証装置。

【請求項２７】

前記受信手段は、前記利用者に関する課金処理に用いられる第３の識別情報をさらに含む前記認証要求を受信する

請求項２５に記載の認証装置。

【請求項２８】

前記個人識別情報は、登録した利用者に予め割り当てられた識別子である

請求項２５に記載の認証装置。

【請求項２９】

前記装置識別情報は、前記装置の製造元で付された当該装置を一意に識別可能な識別子である

請求項２５に記載の認証装置。

【請求項３０】

ネットワークを介して行われる取り引きに関する認証処理を行う認証装置であ

って、

利用者を識別するための個人識別情報と、取り引きの内容を示す取り引き情報と、前記認証要求の送信元の装置を識別する装置識別情報とを含み前記取り引きを行う利用者による前記認証要求を受信する受信手段と、

前記個人識別情報と認証結果を送信する送信先の情報とを対応付けて記憶する記憶手段と、

前記受信した認証要求に含まれる前記取り引き情報を前記認証要求によって指定された利用者の装置に送信し、当該指定された利用者の装置からの応答に応じて、所定の認証処理を行う認証処理手段と、

前記認証要求に含まれる前記個人識別情報に対応する前記送信先の情報を前記記憶手段から読み出し、当該読み出した前記送信先の情報によって特定された送信先に、前記認証処理の結果と、前記認証要求に含まれる前記装置識別情報とを対応付けて送信する送信手段と

を有する認証装置。

【請求項３１】

前記認証処理手段は、

前記取り引き情報に当該認証装置の認証結果を示す署名情報を付して前記指定された利用者の装置に送信し、前記指定された利用者からの応答に応じて、当該認証装置の署名情報を前記認証処理の結果として生成する

請求項３０に記載の認証装置。

【請求項３２】

前記記憶手段は、

前記認証要求を発した利用者と前記指定された利用者との間の取り引きの履歴情報を記憶する

請求項３０に記載の認証装置。

【請求項３３】

前記受信手段は、暗号化された前記個人識別情報および前記装置識別情報を含む前記認証要求を受信し、

前記認証装置は、

前記受信した認証要求に含まれる前記個人識別情報および前記装置識別情報を復号する復号手段

をさらに有する請求項３０に記載の認証装置。

【請求項３４】

前記受信手段は、前記利用者に関する課金処理に用いられる第３の識別情報をさらに含む前記認証要求を受信する

請求項３０に記載の認証装置。

【請求項３５】

前記取り引きに関する認証に対しての課金処理を行う課金処理手段

をさらに有する請求項３０に記載の認証装置。

【請求項３６】

ネットワークを介して行われる取り引きに関する認証要求を行う処理装置であって、

利用者を識別するための個人識別情報と、当該処理装置を識別するための装置識別情報とを含む前記認証要求を送信する送信手段と、

認証要求の送信元の装置を識別するための識別情報を含む認証応答を受信する受信手段と、

前記装置識別情報と、前記認証応答に含まれる識別情報とが一致するか否かを判断する制御手段と

を有する処理装置。

【請求項３７】

前記制御手段は、前記認証応答に含まれる識別情報とが一致しないと判断した場合に、所定の通知を前記認証応答の送信元に通知する

請求項３６に記載の処理装置。

【請求項３８】

前記制御手段は、前記認証応答に含まれる識別情報とが一致しないと判断した場合に、前記認証応答に含まれる当該認証の結果が用いられる取り引き先の装置に所定の通知を行う

請求項３６に記載の処理装置。

【請求項３９】

ネットワークを介して接続される処理装置および認証装置を有する認証システムであって、

前記認証装置は、

利用者を識別するための個人識別情報と、前記認証要求の送信元の装置を識別する装置識別情報とを含む前記認証要求を受信する受信手段と、

前記個人識別情報と認証結果を送信する送信先の情報とを対応付けて記憶する記憶手段と、

前記認証要求に応じて認証処理を行う認証処理手段と、

前記認証要求に含まれる前記個人識別情報に対応する前記送信先の情報を前記記憶手段から読み出し、当該読み出した前記送信先の情報によって特定された送信先に、前記認証処理の結果と前記認証要求に含まれる前記装置識別情報とを含む認証応答を送信する送信手段と

を有し、

前記処理装置は、

前記個人識別情報と、当該処理装置を識別するための前記装置識別情報とを含む前記認証要求を送信する送信手段と、

前記認証応答を受信する受信手段と、

当該処理装置の前記装置識別情報と、前記認証応答に含まれる前記装置識別情報とが一致するか否かを判断する制御手段と

を有する

認証システム。

【請求項４０】

前記制御手段は、前記認証応答に含まれる識別情報とが一致しないと判断した場合に、所定の通知を前記認証応答の送信元に通知する

請求項３９に記載の認証システム。

【請求項４１】

前記制御手段は、前記認証応答に含まれる識別情報とが一致しないと判断した場合に、前記認証応答に含まれる当該認証の結果が用いられる取り引き先の装置

に所定の通知を行う

請求項３９に記載の認証システム。

【請求項４２】

ネットワークを介して接続される処理装置および認証装置を有する認証方法であって、

利用者を識別するための個人識別情報と、当該処理装置を識別するための装置識別情報とを含む認証要求を前記処理装置から前記認証装置に送信し、

前記認証装置において前記認証要求に応じて認証処理を行い、

前記認証装置から、前記認証要求に含まれる前記個人識別情報に対応する前記送信先の情報によって特定された前記処理装置に、前記認証処理の結果と前記認証要求に含まれる前記装置識別情報とを含む認証応答を送信し、

前記処理装置において、前記認証装置から受信した前記認証応答に含まれる前記装置識別情報と、当該処理装置の前記装置識別情報と、前記認証応答に含まれる前記装置識別情報とが一致するか否かを判断する

認証方法。

【請求項４３】

前記処理装置は、前記認証応答に含まれる識別情報とが一致しないと判断した場合に、所定の通知を前記認証装置に通知する

請求項４２に記載の認証方法。

【請求項４４】

前記処理装置は、前記認証応答に含まれる識別情報とが一致しないと判断した場合に、前記認証応答に含まれる当該認証の結果が用いられる取り引き先の装置に所定の通知を行う

請求項４２に記載の認証方法。

【請求項４５】

第１の取り引き者に関する情報を保持し、第２の取り引き者に関する情報を保持する他の認証装置との間で通信を行いながらネットワークを介して行われる前記第１の取り引き者と前記第２の取り引き者との間の取り引きに関する認証を行う認証装置であって、

前記取り引き内容を示す情報と前記第２の取り引き者を特定する情報とを含む前記第１の取り引き者からの第１の要求に応じて、前記第２の取り引き者を特定する情報を含む第２の要求を前記第２の認証装置に送信し、前記第２の要求に応じた前記第２の認証装置による認証結果を示す第１の署名情報を受信し、前記第１の要求に含まれる前記取り引き内容に関する情報と前記第１の署名情報とを含む第３の要求を前記第２の取り引き者が使用する装置に送信し、当該第３の要求に応じて前記第２の取り引き者が使用する装置から所定の応答を受ける送受信手段と、

前記所定の応答を受けた場合に、前記取り引きの履歴を記憶する記憶手段と、

前記所定の応答を受けた場合に、前記送受信手段を介して前記第１の取り引き者が使用する装置に送信される第２の署名情報であって、前記取り引きの正当性の認証結果を示す第２の署名情報を作成する署名作成手段と

を有する認証装置。

【請求項４６】

暗号化手段

をさらに有し、

前記送受信手段は、前記第２の取り引き者との間の通信に用いる暗号鍵を前記第２の要求に応じて前記他の認証装置から受信し、前記暗号化手段で前記暗号鍵を用いて暗号化された前記取り引き内容に関する情報と前記第１の署名情報とを、前記第２の取り引き者が使用する装置に送信する

請求項４５に記載の認証装置。

【請求項４７】

前記送受信手段は、

前記他の認証装置が前記第２の取り引き者を識別するために用いる識別情報を含む前記所定の応答を前記第２の取り引き者が使用する装置から受け、

前記記憶手段は、前記識別情報を用いて生成された前記取り引きの履歴を記憶する

請求項４５に記載の認証装置。

【請求項４８】

前記送受信手段は、前記第１の要求に含まれる前記取り引き内容に関する情報のうち、前記第１の取り引き者の課金に係わる情報以外の情報と、前記第１の署名情報とを含む第３の要求を前記第２の取り引き者が使用する装置に送信する

請求項４５に記載の認証装置。

【請求項４９】

前記送受信手段は、前記第１の要求に含まれる前記取り引き内容に関する情報と、前記第１の署名情報と、当該認証装置との間の通信に用いる暗号鍵とを含む第３の要求を前記第２の取り引き者が使用する装置に送信する

請求項４５に記載の認証装置。

【請求項５０】

前記取り引きに関する認証に対しての課金処理を行う課金処理手段

をさらに有する請求項４５に記載の認証装置。

【請求項５１】

前記課金処理手段は、前記他の認証装置との間で、前記取り引きに関する認証に対して行う課金の割合を決定するための処理を行う

請求項５０に記載の認証装置。

【請求項５２】

前記送受信手段は、前記第２の取り引き者が前記第１の署名情報の正当性を確認して、当該取り引きに同意した場合に、前記第２の取り引き者が使用する装置から、前記記所定の応答を受ける

請求項４５に記載の認証装置。

【請求項５３】

前記送受信手段は、

前記第２の署名情報を前記第２の取り引き者が使用する装置に送信する

請求項４５に記載の認証装置。

【請求項５４】

ネットワークを介して少なくとも２者間で行われた取り引きを認証する認証システムにおいて、

第１の取り引き者に関する取り引きを認証する第１の認証装置と、

第２の取り引き者に関する取り引きを認証する第２の認証装置と

を有し、

前記第１の認証装置は、

前記取り引き内容を示す情報と前記第２の取り引き者を特定する情報とを含む前記第１の取り引き者による第１の要求に応じて、前記第２の取り引き者を特定する情報を含む第２の要求を前記第２の認証装置に送信し、前記第２の要求に応じた前記第２の認証装置による認証結果である第１の署名情報を受信し、前記第１の要求に含まれる前記取り引き内容に関する情報と前記第１の署名情報とを含む第３の要求を前記第２の取り引き者が使用する装置に送信し、当該第３の要求に応じて前記第２の取り引き者から所定の応答を受けると、前記取り引きの履歴を記憶し、前記取り引きの正当性の認証結果を示す第２の署名情報を前記第１の取り引き者に提供する

認証システム。

【請求項５５】

前記第１の認証装置は、

暗号化手段

をさらに有し、

前記送受信手段は、前記第２の取り引き者との間の通信に用いる暗号鍵を前記第２の要求に応じて前記第２の認証装置から受信し、前記暗号化手段で前記暗号鍵を用いて暗号化された前記取り引き内容に関する情報と前記第１の署名情報とを、前記第２の取り引き者が使用する装置に送信する

請求項５４に記載の認証システム。

【請求項５６】

前記第１の認証装置の前記送受信手段は、

前記第２の認証装置が前記第２の取り引き者を識別するために用いる識別情報を含む前記所定の応答を前記第２の取り引き者が使用する装置から受け、

前記記憶手段は、前記識別情報を用いて生成された前記取り引きの履歴を記憶する

請求項５４に記載の認証システム。

【請求項５７】

前記第１の認証装置は、

前記第２の署名情報を前記第２の取り引き者に提供する

請求項５４に記載の認証システム。

【請求項５８】

第１の取り引き者に関する取り引きを認証する第１の認証装置と、第２の取り引き者に関する取り引きを認証する第２の認証装置とを用いて、ネットワークを介して行われる前記第１の取り引き者と前記第２の取り引き者との間の取り引きに関する認証を行う認証方法であって、

前記第１の取り引き者から前記第１の認証装置に、前記取り引き内容を示す情報と前記第２の取り引き者を特定する情報とを含む第１の要求を出し、

前記第１の要求に応じて、前記第１の認証装置から前記第２の認証装置に、前記第２の取り引き者を特定する情報を含む第２の要求を送信し、

前記第２の要求に応じて、前記第２の認証装置からの前記第１の認証装置に、当該第２の認証装置による認証結果を示す第１の署名情報を送信し、

前記第１の認証装置から前記第２の取り引き者が使用する装置に、前記第１の要求に含まれる前記取り引き内容に関する情報と前記第１の署名情報とを含む第３の要求を送信し、

当該第３の要求に応じて、前記第２の取り引き者が使用する装置から前記第１の認証装置に所定の応答を出し、

前記所定の応答に応じて、前記第１の認証装置は、前記取り引きの履歴を記憶し、前記取り引きの正当性の認証結果を示す第２の署名情報を作成し、当該第２の署名情報を、前記第１の取り引き者が使用する装置に送信する

認証方法。

【請求項５９】

前記第２の取り引き者との間の通信に用いる暗号鍵を前記第２の要求に応じて、前記第２の認証装置から前記第１の認証装置に送信し、

前記第１の認証装置は、前記取り引き内容に関する情報と前記第１の署名情報とを、前記暗号鍵を用いて暗号化した後に、前記第２の取り引き者が使用する装

置に送信する

請求項５８に記載の認証方法。

【請求項６０】

前記第１の認証装置は、前記第２の認証装置が前記第２の取り引き者を識別するために用いる識別情報を含む前記所定の応答を前記第２の取り引き者が使用する装置から受け、前記識別情報を用いて生成された前記取り引きの履歴を記憶する

請求項５８に記載の認証方法。

【請求項６１】

前記第１の要求に含まれる前記取り引き内容に関する情報のうち、前記第１の取り引き者の課金に係わる情報以外の情報と、前記第１の署名情報とを含む第３の要求を、前記第１の認証装置から前記第２の取り引き者が使用する装置に送信する

請求項５８に記載の認証方法。

【請求項６２】

前記第１の要求に含まれる前記取り引き内容に関する情報と、前記第１の署名情報と、当該認証装置との間の通信に用いる暗号鍵とを含む第３の要求を、前記第１の認証装置から前記第２の取り引き者が使用する装置に送信する

請求項５８に記載の認証方法。

【請求項６３】

前記第１の認証装置と前記第２の認証装置との間で、前記取り引きに関する認証に対して行う課金の割合を決定するための処理を行う

請求項５８に記載の認証方法。

【請求項６４】

前記第２の取り引き者が前記第１の署名情報の正当性を確認して、当該取り引きに同意した場合に、前記第２の取り引き者が使用する装置から前記第１の認証装置に、前記所定の応答を出す

請求項５８に記載の認証方法。

【請求項６５】

前記第１の認証装置から前記第２の取り引き者が使用する装置に、前記第２の署名情報を送信する

請求項５８に記載の認証方法。

【請求項６６】

利用者を識別するための個人識別情報を含む要求を受信する受信手段と、

前記個人識別情報と処理結果を送信する送信先の情報とを対応付けて記憶する記憶手段と、

前記要求に応じて所定の処理を行う処理手段と、

前記要求に含まれる前記個人識別情報に対応する前記送信先の情報を前記記憶手段から読み出し、当該読み出した前記送信先の情報によって特定された送信先に、前記処理の結果を送信する送信手段と

を有する通信装置。

【請求項６７】

前記受信手段は、暗号化された前記個人識別情報を含む前記要求を受信し、

前記通信装置は、

前記受信した要求に含まれる前記個人識別情報を復号する復号手段

をさらに有する請求項６６に記載の通信装置。

【請求項６８】

前記個人識別情報は、当該通信装置に登録された利用者に予め割り当てられた識別子である

請求項６６に記載の通信装置。

【請求項６９】

前記処理の結果を送信する送信先の情報は、前記要求の送信元がオフラインで当該通信装置に提供した情報である

請求項６６に記載の通信装置。

【請求項７０】

前記所定の結果を送信する送信先の情報は、当該通信装置が接続されるネットワークにおいて、前記利用者を一意に識別するための個人識別情報である

請求項６６に記載の通信装置。

【請求項７１】

前記処理は、認証処理である

請求項６６に記載の通信装置。

【請求項７２】

ネットワークを介して接続される第１の通信装置および第２の通信装置を有する通信システムであって、

前記第１の通信装置は、

利用者を識別するための個人識別情報を含む要求を受信する第１の受信手段と、

前記個人識別情報と処理の結果を送信する送信先の情報とを対応付けて記憶する記憶手段と、

前記要求に応じて所定の処理を行う処理手段と、

前記要求に含まれる前記個人識別情報に対応する前記送信先の情報を前記記憶手段から読み出し、当該読み出した前記送信先の情報によって特定された送信先に、前記処理の結果を送信する第１の送信手段と

を有し、

前記第２の通信装置は、

前記要求を前記第１の通信装置に送信する第２の送信手段と、

前記処理の結果を前記第１の通信装置から受信する第２の受信手段と、

当該受信した認証処理の結果を出力する出力手段と

を有する

通信システム。

【請求項７３】

前記第１の通信装置の前記第１の受信手段は、暗号化された前記個人識別情報を含む前記要求を受信し、

前記第１の通信装置は、

前記受信した要求に含まれる前記個人識別情報を復号する復号手段

をさらに有する請求項７２に記載の通信システム。

【請求項７４】

前記個人識別情報は、当該第１の通信装置に登録された利用者に予め割り当てられた識別子である

請求項７２に記載の通信システム。

【請求項７５】

前記処理の結果を送信する送信先の情報は、前記第２の通信装置の利用者がオフラインで当該第１の通信装置に提供した情報である

請求項７２に記載の通信システム。

【請求項７６】

前記処理の結果を送信する送信先の情報は、前記第１の通信装置が接続されるネットワークにおいて、前記利用者を一意に識別するための個人識別情報である

請求項７２に記載の通信システム。

【請求項７７】

ネットワークを介して接続される第１の通信装置および第２の通信装置を用いた通信方法であって、

利用者を識別するための個人識別情報を含む要求を、前記第２の通信装置から前記第１の通信装置に送信し、

前記第１の通信装置において、前記要求に応じて所定の処理を行い、

前記第１の通信装置は、予め用意された前記個人識別情報と処理の結果を送信する送信先の情報とを対応関係を参照し、前記要求に含まれる前記個人識別情報に対応する送信先の情報によって特定される送信先に、前記処理の結果を送信する

通信方法。

【請求項７８】

前記第２の通信装置において前記第１の通信装置から受信した前記処理の結果を出力する

請求項７７に記載の通信方法。

【請求項７９】

前記第１の通信装置は、暗号化された前記個人識別情報を含む前記要求を受信し、当該受信した要求に含まれる前記個人識別情報を復号する

請求項７７に記載の通信方法。

【請求項８０】

前記個人識別情報は、当該第１の通信装置に登録された利用者に予め割り当てられた識別子である

請求項７７に記載の通信方法。

【請求項８１】

前記処理の結果を送信する送信先の情報は、前記要求の送信元がオフラインで当該第１の通信装置に提供した情報である

請求項７７に記載の通信方法。

【請求項８２】

前記処理の結果を送信する送信先の情報は、前記第１の通信装置が接続されるネットワークにおいて、前記利用者を一意に識別するための個人識別情報である

請求項７７に記載の通信方法。

【請求項８３】

単数または複数の第１の通信装置からの要求に応じてネットワーク上の第２の通信装置で処理を行うことに関しての通信を制御する通信制御装置であって、

前記第１の通信装置を識別するための装置識別情報を記憶する記憶手段と、

前記第１の通信装置からの要求に応じて、当該第１の通信装置に対応する前記装置識別情報を含む要求を前記第２の通信装置に送信する送信手段と、

前記要求の送信元の装置を識別するための装置識別情報を含む応答を前記第２の通信装置から受信する受信手段と、

前記応答に含まれる前記装置識別情報と前記記憶手段に記憶された前記装置識別情報とが一致するか否かに基づいて、前記受信した応答に対応した前記要求が、前記記憶手段に前記装置識別情報が記憶されている正当な前記第１の通信装置によるものであるかを判断する制御手段と

を有する通信制御装置。

【請求項８４】

前記制御手段は、

前記応答に含まれる前記装置識別情報と前記記憶手段に記憶された前記装置識

別情報とが一致しない場合に、前記第２の通信装置に所定の通知を行う

請求項８３に記載の通信制御装置。

【請求項８５】

前記制御手段は、

前記応答に含まれる装置識別情報と前記記憶手段に記憶された前記装置識別情報とが一致しない場合に、前記応答に含まれる処理の結果が用いられる取り引き先の装置に所定の通知を行う

請求項８３に記載の通信制御装置。

【請求項８６】

前記送信手段は、

前記第１の通信装置から受信した個人識別情報と、当該第１の通信装置に対応する前記装置識別情報とを含む前記要求を前記第２の通信装置に送信する

請求項８３に記載の通信制御装置。

【請求項８７】

前記記憶手段は、

前記第１の通信装置から受信した前記装置識別情報を記憶する

請求項８３に記載の通信制御装置。

【請求項８８】

前記記憶手段は、

当該通信制御装置の電源が投入されたときに前記第１の通信装置から受信した前記装置識別情報を記憶する

請求項８７に記載の通信制御装置。

【請求項８９】

前記制御手段は、

前記第１の通信装置と前記第２の通信装置との間の通信履歴を前記記憶手段に書き込む

請求項８３に記載の通信制御装置。

【請求項９０】

前記制御手段は、

前記応答に含まれる前記第２の通信装置の処理結果を、前記要求の送信元の前記第１の通信装置に送信する

請求項８３に記載の通信制御装置。

【請求項９１】

前記制御手段は、

前記受信手段から受信した情報に応じて、待機状態にある前記第１の通信装置が動作状態になるように制御する

請求項８３に記載の通信制御装置。

【請求項９２】

前記制御手段は、

前記第１の通信装置が接続されたネットワークと、前記第２の通信装置が接続されたネットワークとの間の通信を制御する

請求項８３に記載の通信制御装置。

【請求項９３】

前記制御手段は、

ゲートウェイとしての処理を行う

請求項９２に記載の通信制御装置。

【請求項９４】

前記装置識別情報は、前記第１の通信装置の製造元で付された当該通信装置を一意に識別可能な識別子である

請求項８３に記載の通信制御装置。

【請求項９５】

前記個人識別情報は、登録した利用者に予め割り当てられた識別子である

請求項８６に記載の通信制御装置。

【請求項９６】

前記受信手段は、

前記第２の通信装置が行った認証処理の結果を含む前記応答を前記第２の通信装置から受信する

請求項８３に記載の通信制御装置。

【請求項９７】

単数または複数の第１の通信装置からの要求に応じてネットワーク上の第２の通信装置で処理を行うことに関する通信を通信制御装置で制御する通信システムであって、

前記通信制御装置は、

前記第１の通信装置を識別するための装置識別情報を記憶する第１の記憶手段と、

前記第１の通信装置からの要求に応じて、当該第１の通信装置に対応する前記装置識別情報と個人識別情報とを含む要求を前記第２の通信装置に送信する第１の送信手段と、

前記要求の送信元の装置を識別するための装置識別情報を含む応答を前記第２の通信装置から受信する第１の受信手段と、

前記応答に含まれる前記装置識別情報と前記第１の記憶手段に記憶された前記装置識別情報とが一致するか否かに基づいて、前記受信した応答に対応した前記要求が、前記第１の記憶手段に前記装置識別情報が記憶されている正当な前記第１の通信装置によるものであるかを判断する制御手段と

を有し、

前記第２の通信装置は、

前記要求を受信する第２の受信手段と、

前記個人識別情報と処理結果を送信する送信先の情報とを対応付けて記憶する第２の記憶手段と、

前記要求に応じて所定の処理を行う処理手段と、

前記要求に含まれる前記個人識別情報に対応する前記送信先の情報を前記第２の記憶手段から読み出し、当該読み出した前記送信先の情報によって特定された送信先に、前記処理の結果と前記要求に含まれる前記装置識別情報とを対応付けて送信する第２の送信手段と

を有する

通信システム。

【請求項９８】

単数または複数の第１の通信装置からの要求に応じてネットワーク上の第２の通信装置で処理を行うことに関する通信を通信制御装置で制御する通信方法であって、

前記第１の通信装置から前記通信制御装置に出された要求に応じて、当該第１の通信装置に対応する装置識別情報と個人識別情報とを含む要求を前記通信制御装置から前記第２の通信装置に送信し、

前記第２の通信装置において、受信した前記要求に応じた所定の処理を行い、

前記第２の通信装置において、前記要求に含まれる前記個人識別情報に対応する送信先の情報に基づいて、前記処理の結果と前記要求に含まれる前記装置識別情報とを含む応答を前記通信制御装置に送信し、

前記通信制御装置において、受信した前記応答に含まれる前記装置識別情報と、予め保持した前記第１の通信装置の前記装置識別情報とが一致するか否かに基づいて、前記受信した応答に対応した前記要求が、正当な前記第１の通信装置によるものであるかを判断する

通信方法。

【請求項９９】

前記通信制御装置は、

前記応答に含まれる前記装置識別情報と予め保持した前記第１の通信装置の前記装置識別情報とが一致しない場合に、前記第２の通信装置に所定の通知を行う

請求項９８に記載の通信方法。

【請求項１００】

前記通信制御装置は、

前記応答に含まれる前記装置識別情報と予め保持した前記第１の通信装置の前記装置識別情報とが一致しない場合に、前記応答に含まれる処理の結果が用いられる取り引き先の装置に所定の通知を行う

請求項９８に記載の通信方法。

【請求項１０１】

それぞれ単独では所定の情報の秘匿性が保持される複数のモジュールに前記所定の情報を分割し、

前記複数のモジュールを相互に異なる記録媒体または同一の記録媒体の異なる領域に記録する

情報記録方法。

【請求項１０２】

前記複数のモジュールが記録される相互に異なる複数の記録媒体は、物理的に相互に独立している記録媒体である

請求項１０１に記載の情報記録方法。

【請求項１０３】

前記所定の情報を暗号化し、

当該暗号化によって得た情報を、それぞれ単独では所定の情報の秘匿性が保持される前記複数のモジュールに分割する

請求項１０１に記載の情報記録方法。

【請求項１０４】

前記複数のモジュールをそれぞれ暗号化し、

当該暗号化によって得られた複数のモジュールを相互に異なる記録媒体または同一の記録媒体の異なる領域に記録する

請求項１０１に記載の情報記録方法。

【請求項１０５】

それぞれ単独では所定の情報の秘匿性が保持される複数のモジュールが相互に異なる複数の記録媒体または同一の記録媒体の異なる領域に記録されている場合に、前記複数の記録媒体または同一の記録媒体の異なる領域からそれぞれ前記モジュールを読み出し、

当該読み出したモジュールを合成して前記所定の情報を復元する

情報復元方法。

【請求項１０６】

前記複数のモジュールが記録される相互に異なる複数の記録媒体は、物理的に相互に独立している記録媒体である

請求項１０５に記載の情報復元方法。

【請求項１０７】

前記読み出したモジュールを合成した後に復号して前記所定の情報を復元する請求項１０５に記載の情報復元方法。

【請求項１０８】

前記読み出したモジュールを復号した後に合成して前記所定の情報を復元する請求項１０５に記載の情報復元方法。

【請求項１０９】

それぞれ単独では所定の情報の秘匿性が保持される複数のモジュールに前記所定の情報を分割する情報分割手段と、

前記複数のモジュールを相互に異なる記録媒体または同一の記録媒体の異なる領域に書き込む書き込み手段と

を有する情報記録装置。

【請求項１１０】

前記複数のモジュールが記録される相互に異なる複数の記録媒体は、物理的に相互に独立している記録媒体である

請求項１０９に記載の情報記録装置。

【請求項１１１】

前記所定の情報を暗号化する暗号化手段

をさらに有し、

前記情報分割手段は、

前記暗号化によって得た情報を、それぞれ単独では所定の情報の秘匿性が保持される前記複数のモジュールに分割する

請求項１０９に記載の情報記録装置。

【請求項１１２】

前記複数のモジュールをそれぞれ暗号化する暗号化手段

をさらに有し、

前記書き込み手段は、

前記暗号化によって得られた複数のモジュールを相互に異なる記録媒体または同一の記録媒体の異なる領域に書き込む

請求項１０９に記載の情報記録装置。

【請求項１１３】

それぞれ単独では所定の情報の秘匿性が保持される複数のモジュールが相互に異なる複数の記録媒体または同一の記録媒体の異なる領域に記録されている場合に、前記複数の記録媒体または同一の記録媒体の異なる領域からそれぞれ前記モジュールを読み出す読み出し手段と、

当該読み出したモジュールを合成して前記所定の情報を復元する情報合成手段と

を有する情報復元装置。

【請求項１１４】

前記複数のモジュールが記録される相互に異なる複数の記録媒体は、物理的に相互に独立している記録媒体である

請求項１１３に記載の情報復元装置。

【請求項１１５】

前記合成して得た情報を復号する復号手段

をさらに有する

請求項１１３に記載の情報復元装置。

【請求項１１６】

前記読み出したモジュールを復号する復号手段

をさらに有し、

前記情報合成手段は、前記復号したモジュールを合成して前記所定の情報を復元する

請求項１１３に記載の情報復元装置。

【請求項１１７】

それぞれ単独では所定の情報の秘匿性が保持される複数のモジュールに前記所定の情報を分割した場合に、前記複数のモジュールのうち一のモジュールが記録された

記録媒体。

【請求項１１８】

認証装置において、ユーザの認証情報を第１の認証情報および第２の認証情報

に分割し、

前記第２の認証情報を記憶した携帯型メモリ装置を前記ユーザに提供し、

前記携帯型メモリ装置にアクセス可能な端末装置から前記認証装置に認証情報要求を送信し、

前記認証装置において、前記認証情報要求が正当なユーザによるものであると判断した場合に、前記認証装置から前記端末装置に前記第１の認証情報を送信し、

前記端末装置において、前記認証装置から受信した前記第１の認証情報と、前記携帯型メモリ装置から読み出した前記第２の認証情報とを用いて前記認証情報を復元する

認証方法。

【請求項１１９】

前記認証情報要求は、前記第１の認証情報の送信先を指定した送信先情報を含み、

前記認証装置は、前記送信先情報で指定された前記端末装置に、前記第１の認証情報を送信する

請求項１１８に記載の認証方法。

【請求項１２０】

前記認証装置は、前記ユーザに対応する送信先情報を予め記憶し、当該記憶した送信先情報内に、前記認証情報要求に含まれる前記送信先情報が存在する場合に、前記認証情報要求が正当なユーザによるものであると判断する

請求項１１９に記載の認証方法。

【請求項１２１】

前記端末装置は、前記認証装置から受信した前記第１の認証情報と、前記携帯型メモリ装置から読み出した前記第２の認証情報とが対応していると判断した場合に、前記受信した第１の認証情報を記憶して前記認証情報を復元する

請求項１１８に記載の認証方法。

【請求項１２２】

前記端末装置は、前記認証装置から受信した前記第１の認証情報と、前記携帯

型メモリ装置から読み出した前記第２の認証情報とが対応していない場合に、その旨を示す通知を前記認証装置に送信する

請求項１１８に記載の認証方法。

【請求項１２３】

前記認証装置は、前記ユーザからの要求に応じて、前記認証情報を生成する

請求項１１８に記載の認証方法。

【請求項１２４】

前記認証情報は、公開鍵暗号を用いて作成された情報である

請求項１１８に記載の認証方法。

【請求項１２５】

前記携帯型メモリ装置は、スマートメディアである

請求項１１８に記載の認証方法。

【請求項１２６】

認証情報を生成し、

前記認証情報を第１の認証情報および第２に認証情報に分割し、

前記第２の認証情報を記憶した携帯型メモリ装置をユーザに提供し、

受信した認証情報要求が正当なユーザによるものであると判断した場合に、前記認証情報要求が指定する送信先に、前記第１の認証情報を送信する

認証方法。

【請求項１２７】

前記ユーザに対応する送信先情報を予め記憶し、

前記記憶した送信先情報内に、前記認証情報要求に含まれる前記送信先情報が存在する場合に、前記認証情報要求が正当なユーザによるものであると判断する

請求項１２６に記載の認証方法。

【請求項１２８】

前記認証情報は、公開鍵暗号を用いて作成された情報である

請求項１２６に記載の認証方法。

【請求項１２９】

前記携帯型メモリ装置は、スマートメディアである

請求項１２６に記載の認証方法。

【請求項１３０】

認証情報を生成し、前記認証情報を第１の認証情報および第２に認証情報に分割し、受信した認証情報要求が正当なユーザによるものであるか否かを判断する制御手段と、

携帯型メモリ装置に前記第２の認証情報を書き込む書込手段と、

前記携帯型メモリ装置のユーザから前記認証情報要求を受信する受信手段と、

前記認証情報要求が正当なユーザによるものであると判断された場合に、前記第１の認証情報を前記認証情報要求によって指定された送信先に送信する送信手段と

を有する認証装置。

【請求項１３１】

前記ユーザに対応する送信先情報を予め記憶する記憶手段

をさらに有し、

前記制御手段は、前記記憶した送信先情報に、前記認証情報要求によって指定された送信先が示されている場合に、前記認証情報要求が正当なユーザによるものであると判断する

請求項１３０に記載の認証装置。

【請求項１３２】

前記認証情報は、公開鍵暗号を用いて作成された情報である

請求項１３０に記載の認証装置。

【請求項１３３】

前記携帯型メモリ装置は、スマートメディアである

請求項１３０に記載の認証装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、他人の個人ＩＤ情報を不正に用いた手続を防止できる認証装置、認証システムおよびその方法、処理装置、通信装置、通信制御装置、通信システム

およびその方法、記録媒体に保持される情報の秘匿性を高めることができる情報記録方法およびその装置、情報復元方法およびその装置並びに記録媒体に関する。

【０００２】

【従来の技術】

インターネットなどのネットワークを介した電子商取引が普及している。

このような電子商取引を用いて利用者が商品等を購入する場合には、例えば、利用者が店舗や各家庭に設置されたパーソナルコンピュータなどの発注者端末装置を操作して、ネットワークを介して、商品等の販売を行う受注者サーバ装置にアクセスを行う。これにより、サーバ装置から発注者端末装置に商品の写真、特性および価格などの情報が提供され、発注者端末装置のディスプレイに表示される。利用者は、このような情報を見ながら、購入を希望する商品等を選択し、選択した商品等の発注処理を行う。発注処理は、利用者個人を特定する個人ＩＤ情報、発注する商品等を指定した情報およびその決済方法等の情報を、発注者端末装置を操作して入力し、これをネットワークを介してサーバ装置に送信する。

【０００３】

また、近年、電子商取り引きの発達に伴い、ユーザの個人ＩＤ情報や暗証番号、取り引きの履歴情報、ユーザの名前、住所、経歴および職業などの個人情報などの秘匿性のある情報を、サーバ装置や端末装置などが管理する場合が多くなっている。

サーバ装置や端末装置では、例えば、特開平１１－２７２６７８１号公報に示されるように、上述したような秘匿性のある情報を、所定の暗号鍵で暗号化して、コンピュータに内蔵されたＨＤＤ(Hard Disk Drive) や、携帯性のあるＣＤ－ＲＯＭ、フロッピーディスク、ＰＣカードなどの記録媒体に記録している。

【０００４】

【発明が解決しようとする課題】

しかしながら、上述したネットワークを介した従来の電子商取引では、発注者および受注者の当事者間でのみ取り引きが行われることから、偽発注および商取引情報の改竄などの不正を取り締まりことが困難であるという問題がある。

また、このような電子商取引について第３者が認証を行う場合でも、他人の個人ＩＤ情報を用いてネットワークを介して行われる不正な手続（いわゆる、なりすまし）が行われる可能性があるという問題がある。

【０００５】

また、上述したような電子商取引が普及すると、複数に認証機関が、電子商取引の認証業務を行うことになる。この場合に、同じ電子商取引に参加した利用者が、それぞれ異なる認証機関と契約をしている場合に、どのようにして当該電子商取引の正当性を認証するかが課題となる。

この場合に、同じ電子商取引に参加した利用者が契約した複数の認証機関で、、利用者の情報を共有することで、上述した課題に対処できるが、利用者の個人情報が、他の機関に漏れてしまうという問題がある。

【０００６】

また、家庭内に複数の端末装置を設けた場合に、外部のネットワークを介して行われる電子商取引やセキュリティに関する機能を端末装置毎に持たせると、効率が悪いと共に、例えば家庭単位で通信履歴を管理するときに不便である。

【０００７】

また、上述した従来のサーバ装置や端末装置では、通常、秘匿性のある情報を単体の記録媒体に記録しており、その記録媒体が盗まれたり、不正にコピーされると、当該情報の秘匿性が失われてしまうという問題がある。

このような秘匿性のある情報は、通常、暗号化されて記録媒体に記録されるが、暗号化は復号（解読）される可能性があり、秘匿性を保持する上で十分ではない。

【０００８】

また、近年、公開鍵暗号方式を用いて生成した個人認証情報（ＰＫＩ情報）をスマートカード（スマートメディア）と称される小型のメモリカードに記憶し、当該メモリカードを用いて個人認証を行う場合があるが、このような個人認証情報は、印鑑証明と同等の効力を有していることから、メモリカードが盗難あるいは紛失された場合の被害が大きいという問題がある。

このような問題を回避するために、メモリカードの使用に際して、パスワード

の照合を行うことが考えられるが、使い勝手が悪いという問題がある。

【０００９】

本発明は上述した従来技術の問題点に鑑みてなされ、不正に取得した他人の個人ＩＤ情報に基づいて不正な手続が行われることを回避する認証装置、認証システムおよびその方法を提供することを目的とする。

【００１０】

また、本発明は、異なる認証機関と契約した利用者相互間の取り引きの認証を、利用者の個人情報を他の認証機関に提供することなく、高い信頼性で行うことができる認証装置、認証システムおよびその方法を提供することを目的とする。

【００１１】

また、本発明は、複数の端末装置を用いてネットワークを介した電子商取引などを行う場合に、当該電子商取引に必要な機能の割り当て、並びに通信履歴の管理を効率的に行うことができる通信制御装置、通信システムおよびその方法を提供することを目的とする。

【００１２】

また、本発明は、情報を高い秘匿性を保ちながら記録媒体に記録できる情報記録方法、情報復元方法およびそれらの装置と記録媒体を提供することを目的とする。

【００１３】

また、本発明は、個人認証機能を持つ携帯型メモリ装置を用いて認証を行う場合に、煩雑な手続きを行うことなく、その安全性を高めることができる認証方法およびその装置を提供することを目的とする。

【００１４】

【課題を解決するための手段】

上述した従来技術の問題点を解決し、上述した目的を達成するために、第１の発明の認証装置は、ネットワークを介して少なくとも２者間で行われる取り引きを認証する認証装置であって、第１の取り引き者の個人識別情報、第２の取り引き者の個人識別情報および取り引き内容を示す情報を含む第１の要求を、前記第１の取り引き者から受信する第１の受信手段と、前記第１の要求に応じて、前記

第１の取り引き者の正当性を認証して第１の認証情報を生成する第１の認証手段と、前記第１の認証情報および前記取り引きの内容を示す情報を含む第２の要求を前記第２の取り引き者に送信する第１の送信手段と、前記第２の要求に対しての応答を前記第２の取り引き者から受信する第２の受信手段と、前記応答に応じて、前記第２の取り引き者の正当性を認証して第２の認証情報を生成する第２の認証手段と、前記第２の認証情報を前記第１の取り引き者に送信する第２の送信手段とを有する。

【００１５】

第１の発明の認証装置の作用は以下のようになる。

第１の受信手段によって、第１の取り引き者の個人識別情報、第２の取り引き者の個人識別情報および取り引き内容を示す情報を含む第１の要求が、前記第１の取り引き者から受信される。

次に、第１の認証装置によって、前記第１の要求に応じて、前記第１の取り引き者の正当性が認証され、第１の認証情報が生成される。

次に、第１の送信手段によって、前記第１の認証情報および前記取り引きの内容を示す情報を含む第２の要求が前記第２の取り引き者に送信される。

そして、第２の受信手段によって、前記第２の要求に対しての応答が前記第２の取り引き者から受信される。

次に、第２の認証手段によって、前記応答に応じて、前記第２の取り引き者の正当性が認証され、第２の認証情報が生成される。

次に、第２の送信手段によって、前記第２の認証情報が前記第１の取り引き者に送信される。

【００１６】

上述したように、第１の発明によれば、第１の取り引き者と第２の取り引き者とが通信を行って取り引きを行う場合に、第１の取り引き者および第２の取り引き者以外の第３者が管理する当該認証装置を用いることで、第１の取り引き者の正当性を客観的に認証した結果である第１の認証情報を第２の取り引き者に送信し、第２の取り引き者の正当性を客観的に認証した結果である第２の認証情報を第１の取り引き者に送信することができ、取り引きの信頼性を高めることが可能

になる。

【００１７】

第１の発明は、好ましくは、前記第１の受信手段は、前記第１の取り引き者の個人キー情報をさらに含む前記第１の要求を受信し、前記第１の認証手段は、前記個人キー情報に基づいて前記第１の取り引き者の正当性を認証し、前記第２の受信手段は、前記第２の取り引き者の個人キー情報を含む前記応答を受信し、前記第１の認証手段は、前記第２の取り引き者の個人キー情報に基づいて前記第２の取り引き者の正当性を認証する。

ここで、前記第１の取り引き者および前記第２の取り引き者の前記個人キー情報は、それぞれ前記第１の取り引き者および前記第２の取り引き者の課金に係わる情報である。

【００１８】

第１の発明の認証装置は、好ましくは、前記第１の送信手段は、前記第１の取り引き者の前記個人キー情報をさらに含む第２の要求を前記第２の取り引き者に送信する。

【００１９】

第１の発明の認証装置は、好ましくは、前記取り引きの履歴を示す履歴情報を記憶する記憶手段をさらに有する。

【００２０】

第２の発明の認証システムは、ネットワークを介して少なくとも２者間で行われる取り引きを認証する認証システムであって、第１の取り引き者が使用する第１の通信装置と、第２の取り引き者が使用する第２の通信装置と、前記取り引きを認証する認証装置とを有し、前記第１の通信装置は、第１の取り引き者の個人識別情報、第２の取り引き者の個人識別情報および取り引き内容を示す情報を含む第１の要求を前記認証装置に送信し、前記認証装置は、前記第１の取り引き者から前記第１の要求を受信する第１の受信手段と、前記第１の要求に応じて、前記第１の取り引き者の正当性を認証して第１の認証情報を生成する第１の認証手段と、前記第１の認証情報および前記取り引きの内容を示す情報を含む第２の要求を前記第２の取り引き者に送信する第１の送信手段と、前記第２の要求に対し

ての応答を前記第２の取り引き者から受信する第２の受信手段と、前記応答に応じて、前記第２の取り引き者の正当性を認証して第２の認証情報を生成する第２の認証手段と、前記第２の認証情報を前記第１の取り引き者に送信する第２の送信手段とを有する。

ここで、第２の発明の認証システムの前記認証装置の作用は前述した第１の発明の認証装置の作用と同じである。

【００２１】

第３の発明の認証方法は、ネットワークを介して少なくとも２者間で行われる取り引きを認証する認証方法であって、第１の取り引き者の個人識別情報、第２の取り引き者の個人識別情報および取り引き内容を示す情報を含む第１の要求を、前記第１の取り引き者から受信し、前記第１の要求に応じて、前記第１の取り引き者の正当性を認証して第１の認証情報を生成し、前記第１の認証情報および前記取り引きの内容を示す情報を含む第２の要求を前記第２の取り引き者に送信し、前記第２の要求に対しての応答を前記第２の取り引き者から受信し、前記応答に応じて、前記第２の取り引き者の正当性を認証して第２の認証情報を生成し、前記第２の認証情報を前記第１の取り引き者に送信する。

【００２２】

第４の発明の認証装置は、ネットワークを介して少なくとも２者間で行われる取り引きを認証する認証装置であって、第１の取り引き者の個人識別情報、前記第１の取り引き者の個人キー情報、第２の取り引き者の個人識別情報および取り引き内容を示す情報を含む第１の要求を、前記第１の取り引き者から受信する第１の受信手段と、前記第１の要求に含まれる前記個人キー情報に基づいて前記第１の取り引き者の正当性を認証して第１の認証情報を生成する第１の認証手段と、前記第１の要求から前記第１の取り引き者の個人キー情報を除去した情報と、前記第１の認証情報とを含む第２の要求を前記第２の取り引き者に送信する第１の送信手段と、前記第２の要求に対しての応答を前記第２の取り引き者から受信する第２の受信手段と、前記応答に応じて、前記第２の取り引き者の正当性を認証して第２の認証情報を生成する第２の認証手段と、前記第２の認証情報を前記第１の取り引き者に送信する第２の送信手段とを有する。

【００２３】

第４の発明の認証装置の作用は以下のようになる。

第１の受信手段によって、第１の取り引き者の個人識別情報、第２の取り引き者の個人識別情報および取り引き内容を示す情報を含む第１の要求が、前記第１の取り引き者から受信される。

次に、第１の認証装置によって、前記第１の要求に応じて、前記第１の取り引き者の正当性が認証され、第１の認証情報が生成される。

次に、第１の送信手段によって、前記第１の要求から前記第１の取り引き者の個人キー情報を除去した情報と、前記第１の認証情報とを含む第２の要求が前記第２の取り引き者に送信される。

そして、第２の受信手段によって、前記第２の要求に対しての応答が前記第２の取り引き者から受信される。

次に、第２の認証手段によって、前記応答に応じて、前記第２の取り引き者の正当性が認証され、第２の認証情報が生成される。

次に、第２の送信手段によって、前記第２の認証情報が前記第１の取り引き者に送信される。

【００２４】

第４の発明の認証装置によれば、第１の送信手段から第２の取り引き者に送信される第２の要求には、前記第１の取り引き者の個人キー情報が含まれていないため、第２の取り引き者に、第１の取り引き者の課金に係わる情報が漏れることを回避できる。

【００２５】

第４の発明の認証装置は、好ましくは、前記第２の受信手段は、前記第２の取り引き者の個人キー情報を含む前記応答を受信し、前記第１の認証手段は、前記第２の取り引き者の個人キー情報に基づいて前記第２の取り引き者の正当性を認証する。

ここで、前記第１の取り引き者の個人キー情報は前記第１の取り引き者の課金に係わる情報であり、前記第２の取り引き者の個人キー情報は前記第２の取り引き者の課金に係わる情報である。

【００２６】

第５の発明の認証システムは、ネットワークを介して少なくとも２者間で行われる取り引きを認証する認証システムであって、第１の取り引き者が使用する第１の通信装置と、第２の取り引き者が使用する第２の通信装置と、前記取り引きを認証する認証装置とを有し、前記認証装置は、第１の取り引き者の個人識別情報、前記第１の取り引き者の個人キー情報、第２の取り引き者の個人識別情報および取り引き内容を示す情報を含む第１の要求を、前記第１の取り引き者から受信する第１の受信手段と、前記第１の要求に含まれる前記個人キー情報に基づいて前記第１の取り引き者の正当性を認証して第１の認証情報を生成する第１の認証手段と、前記第１の要求から前記第１の取り引き者の個人キー情報を除去した情報と、前記第１の認証情報とを含む第２の要求を前記第２の取り引き者に送信する第１の送信手段と、前記第２の要求に対しての応答を前記第２の取り引き者から受信する第２の受信手段と、前記応答に応じて、前記第２の取り引き者の正当性を認証して第２の認証情報を生成する第２の認証手段と、前記取り引きの正当性を示す第２の認証情報を前記第１の取り引き者に送信する第２の送信手段とを有する。

【００２７】

第５の発明の認証システムの前記認証装置の作用は前述した第４の発明の認証装置の作用と同じである。

【００２８】

第６の発明の認証方法は、ネットワークを介して少なくとも２者間で行われる取り引きを認証する認証方法であって、第１の取り引き者の個人識別情報、前記第１の取り引き者の個人キー情報、第２の取り引き者の個人識別情報および取り引き内容を示す情報を含む第１の要求を、前記第１の取り引き者から受信し、前記第１の要求に含まれる前記個人キー情報に基づいて前記第１の取り引き者の正当性を認証して第１の認証情報を生成し、前記第１の要求から前記第１の取り引き者の個人キー情報を除去した情報と、前記第１の認証情報とを含む第２の要求を前記第２の取り引き者に送信し、前記第２の要求に対しての応答を前記第２の取り引き者から受信し、前記応答に応じて、前記第２の取り引き者の正当性を認

証して第２の認証情報を生成し、前記第２の認証情報を前記第１の取り引き者に送信する。

【００２９】

第７の発明の認証装置は、認証要求に応じて認証処理を行う認証装置であって、利用者を識別するための個人識別情報と、前記認証要求の送信元の装置を識別する装置識別情報とを含む前記認証要求を受信する受信手段と、前記個人識別情報と認証結果を送信する送信先の情報とを対応付けて記憶する記憶手段と、前記認証要求に応じて認証処理を行う認証処理手段と、前記認証要求に含まれる前記個人識別情報に対応する前記送信先の情報を前記記憶手段から読み出し、当該読み出した前記送信先の情報によって特定された送信先に、前記認証処理の結果と前記認証要求に含まれる前記装置識別情報とを対応付けて送信する送信手段とを有する。

【００３０】

第７の発明の認証装置の作用は以下のようになる。

例えば、利用者が端末装置などを操作して当該端末装置から送信された、利用者を識別するための個人識別情報と、認証要求の送信元の装置を識別する装置識別情報とを含む前記認証要求が受信手段で受信される。

次に、当該受信された前記認証要求に応じた認証処理が認証処理手段で行われる。

次に、送信手段によって、前記認証要求に含まれる前記個人識別情報に対応する前記送信先の情報が記憶手段から読み出され、当該読み出された前記送信先の情報によって特定された送信先に、前記認証処理の結果と前記認証要求に含まれる前記装置識別情報とが対応付けて送信手段から送信される。

【００３１】

第７の発明の認識装置は、好ましくは、前記受信手段は、暗号化された前記個人識別情報および前記装置識別情報を含む前記認証要求を受信し、前記認証装置は、前記受信した認証要求に含まれる前記個人識別情報および前記装置識別情報を復号する復号手段をさらに有する。

また、第７の発明の認証装置は、好ましくは、前記受信手段は、前記利用者に

関する課金処理に用いられる第３の識別情報をさらに含む前記認証要求を受信する。

また、第７の発明の認証装置は、好ましくは、前記個人識別情報は、登録した利用者に予め割り当てられた識別子である。

また、第７の発明の認証装置は、好ましくは、前記装置識別情報は、前記装置の製造元で付された当該装置を一意に識別可能な識別子である。

【００３２】

第８の発明の認証装置は、ネットワークを介して行われる取り引きに関する認証処理を行う認証装置であって、利用者を識別するための個人識別情報と、取り引きの内容を示す取り引き情報と、前記認証要求の送信元の装置を識別する装置識別情報とを含み前記取り引きを行う利用者による前記認証要求を受信する受信手段と、前記個人識別情報と認証結果を送信する送信先の情報とを対応付けて記憶する記憶手段と、前記受信した認証要求に含まれる前記取り引き情報を前記認証要求によって指定された利用者の装置に送信し、当該指定された利用者の装置からの応答に応じて、所定の認証処理を行う認証処理手段と、前記認証要求に含まれる前記個人識別情報に対応する前記送信先の情報を前記記憶手段から読み出し、当該読み出した前記送信先の情報によって特定された送信先に、前記認証処理の結果と、前記認証要求に含まれる前記装置識別情報とを対応付けて送信する送信手段とを有する。

【００３３】

第８の発明の認証装置の作用は以下のようになる。

利用者を識別するための個人識別情報と、取り引きの内容を示す取り引き情報と、前記認証要求の送信元の装置を識別する装置識別情報とを含み前記取り引きを行う利用者による前記認証要求が受信手段で受信される。

次に、認証処理手段によって、前記受信した認証要求に含まれる前記取り引き情報が前記認証要求によって指定された利用者の装置に送信され、当該指定された利用者の装置からの応答に応じて、所定の認証処理が行われる。

次に、送信手段によって、前記認証要求に含まれる前記個人識別情報に対応する前記送信先の情報が記憶手段から読み出され、当該読み出された前記送信先の

情報によって特定された送信先に、前記認証処理の結果と、前記認証要求に含まれる前記装置識別情報とを対応付けて送信手段から送信される。

【００３４】

第８の発明の認証装置は、好ましくは、前記認証処理手段は、前記取り引き情報に当該認証装置の認証結果を示す署名情報を付して前記指定された利用者の装置に送信し、前記指定された利用者からの応答に応じて、当該認証装置の署名情報を前記認証処理の結果として生成する。

【００３５】

第８の発明の認証装置は、好ましくは、前記記憶手段は、前記認証要求を発した利用者と前記指定された利用者との間の取り引きの履歴情報を記憶する。

【００３６】

第８の発明の認証装置は、好ましくは、前記受信手段は、暗号化された前記個人識別情報および前記装置識別情報を含む前記認証要求を受信し、前記認証装置は、前記受信した認証要求に含まれる前記個人識別情報および前記装置識別情報を復号する復号手段をさらに有する。

【００３７】

また、第８の発明の認証装置は、好ましくは、前記受信手段は、前記利用者に関する課金処理に用いられる第３の識別情報をさらに含む前記認証要求を受信する。

また、第８の発明の認証装置は、好ましくは、前記取り引きに関する認証に対しての課金処理を行う課金処理手段をさらに有する。

【００３８】

第９の発明の処理装置は、ネットワークを介して行われる取り引きに関する認証要求を行う処理装置であって、利用者を識別するための個人識別情報と、当該処理装置を識別するための装置識別情報とを含む前記認証要求を送信する送信手段と、認証要求の送信元の装置を識別するための識別情報を含む認証応答を受信する受信手段と、前記装置識別情報と、前記認証応答に含まれる識別情報とが一致するか否かを判断する制御手段とを有する。

【００３９】

第９の発明の処理装置は、好ましくは、前記制御手段は、前記認証応答に含まれる識別情報とが一致しないと判断した場合に、所定の通知を前記認証応答の送信元に通知する。

また、第９の発明の処理装置は、好ましくは、前記制御手段は、前記認証応答に含まれる識別情報とが一致しないと判断した場合に、前記認証応答に含まれる当該認証の結果が用いられる取り引きの取り引き先の装置に所定の通知を行う。

【００４０】

第１０の発明の認証システムは、ネットワークを介して接続される処理装置および認証装置を有する認証システムであって、前記認証装置は、利用者を識別するための個人識別情報と、前記認証要求の送信元の装置を識別する装置識別情報とを含む前記認証要求を受信する受信手段と、前記個人識別情報と認証結果を送信する送信先の情報とを対応付けて記憶する記憶手段と、前記認証要求に応じて認証処理を行う認証処理手段と、前記認証要求に含まれる前記個人識別情報に対応する前記送信先の情報を前記記憶手段から読み出し、当該読み出した前記送信先の情報によって特定された送信先に、前記認証処理の結果と前記認証要求に含まれる前記装置識別情報とを含む認証応答を送信する送信手段とを有し、前記処理装置は、前記個人識別情報と、当該処理装置を識別するための前記装置識別情報とを含む前記認証要求を送信する送信手段と、前記認証応答を受信する受信手段と、当該処理装置の前記装置識別情報と、前記認証応答に含まれる前記装置識別情報とが一致するか否かを判断する制御手段とを有する。

【００４１】

第１１の発明の認証方法は、ネットワークを介して接続される処理装置および認証装置を有する認証方法であって、利用者を識別するための個人識別情報と、当該処理装置を識別するための装置識別情報とを含む認証要求を前記処理装置から前記認証装置に送信し、前記認証装置において前記認証要求に応じて認証処理を行い、前記認証装置から、前記認証要求に含まれる前記個人識別情報に対応する前記送信先の情報によって特定された前記処理装置に、前記認証処理の結果と前記認証要求に含まれる前記装置識別情報とを含む認証応答を送信し、前記処理装置において、前記認証装置から受信した前記認証応答に含まれる前記装置識別

情報と、当該処理装置の前記装置識別情報と、前記認証応答に含まれる前記装置識別情報とが一致するか否かを判断する。

【００４２】

第１２の発明の認証装置は、第１の取り引き者に関する情報を保持し、第２の取り引き者に関する情報を保持する他の認証装置との間で通信を行いながらネットワークを介して行われる前記第１の取り引き者と前記第２の取り引き者との間の取り引きに関する認証を行う認証装置であって、前記取り引き内容を示す情報と前記第２の取り引き者を特定する情報とを含む前記第１の取り引き者からの第１の要求に応じて、前記第２の取り引き者を特定する情報を含む第２の要求を前記第２の認証装置に送信し、前記第２の要求に応じた前記第２の認証装置による認証結果を示す第１の署名情報を受信し、前記第１の要求に含まれる前記取り引き内容に関する情報と前記第１の署名情報とを含む第３の要求を前記第２の取り引き者が使用する装置に送信し、当該第３の要求に応じて前記第２の取り引き者が使用する装置から所定の応答を受ける送受信手段と、前記所定の応答を受けた場合に、前記取り引きの履歴を記憶する記憶手段と、前記所定の応答を受けた場合に、前記送受信手段を介して前記第１の取り引き者が使用する装置に送信される第２の署名情報であって、前記取り引きの正当性の認証結果を示す第２の署名情報を作成する署名作成手段とを有する。

【００４３】

第１２の発明の認証装置の作用は以下のようになる。

送受信手段、前記取り引き内容を示す情報と前記第２の取り引き者を特定する情報とを含む前記第１の取り引き者からの第１の要求を受ける。

そして、当該第２の要求に応じて、前記第２の取り引き者を特定する情報を含む第２の要求が、前記送受信手段から前記第２の認証装置に送信される。

次に、送受信手段は、前記第２の要求に応じた第１の署名情報を前記第２の認証装置から受信する。

次に、前記第１の要求に含まれる前記取り引き内容に関する情報と前記第１の署名情報とを含む第３の要求を、前記送受信手段から前記第２の取り引き者が使用する装置に送信する。

次に、送受信手段は、当該第３の要求に応じて前記第２の取り引き者が使用する装置から所定の応答を受ける。

前記送受信手段が前記所定の応答を受けると、記憶手段に、前記取り引きの履歴が記憶される。

また、前記送受信手段が前記所定の応答を受けると、署名作成手段によって、前記取り引きの正当性を認証する第２の署名情報が作成され、当該第２の署名情報が、前記送受信手段を介して前記第１の取り引き者が使用する装置に送信される。

【００４４】

第１２の発明の認証装置は、好ましくは、暗号化手段をさらに有し、前記送受信手段は、前記第２の取り引き者との間の通信に用いる暗号鍵を前記第２の要求に応じて前記他の認証装置から受信し、前記暗号化手段で前記暗号鍵を用いて暗号化された前記取り引き内容に関する情報と前記第１の署名情報とを、前記第２の取り引き者が使用する装置に送信する。

【００４５】

第１２の発明の認証装置は、好ましくは、前記送受信手段は、前記他の認証装置が前記第２の取り引き者を識別するために用いる識別情報を含む前記所定の応答を前記第２の取り引き者が使用する装置から受け、前記記憶手段は、前記識別情報を用いて生成された前記取り引きの履歴を記憶する。

【００４６】

第１２の発明の認証装置は、好ましくは、前記送受信手段は、前記第１の要求に含まれる前記取り引き内容に関する情報のうち、前記第１の取り引き者の課金に係わる情報以外の情報と、前記第１の署名情報とを含む第３の要求を前記第２の取り引き者が使用する装置に送信する。

【００４７】

第１２の発明の認証装置は、好ましくは、前記送受信手段は、前記第１の要求に含まれる前記取り引き内容に関する情報と、前記第１の署名情報と、当該認証装置との間の通信に用いる暗号鍵とを含む第３の要求を前記第２の取り引き者が使用する装置に送信する。

【００４８】

第１２の発明の認証装置は、好ましくは、前記取り引きに関する認証に対しての課金処理を行う課金処理手段をさらに有する。

【００４９】

第１２の発明の認証装置は、好ましくは、前記課金処理手段は、前記他の認証装置との間で、前記取り引きに関する認証に対して行う課金の割合を決定するための処理を行う。

【００５０】

第１２の発明の認証装置は、好ましくは、前記送受信手段は、前記第２の取り引き者が前記第１の署名情報の正当性を確認して、当該取り引きに同意した場合に、前記第２の取り引き者が使用する装置から、前記記所定の応答を受ける。

【００５１】

第１３の発明の認証システムは、ネットワークを介して少なくとも２者間で行われた取り引きを認証する認証システムであって、第１の取り引き者に関する取り引きを認証する第１の認証装置と、第２の取り引き者に関する取り引きを認証する第２の認証装置とを有し、前記第１の認証装置は、前記取り引き内容を示す情報と前記第２の取り引き者を特定する情報とを含む前記第１の取り引き者による第１の要求に応じて、前記第２の取り引き者を特定する情報を含む第２の要求を前記第２の認証装置に送信し、前記第２の要求に応じた前記第２の認証装置からの第１の署名情報を受信し、前記第１の要求に含まれる前記取り引き内容に関する情報と前記第１の署名情報とを含む第３の要求を前記第２の取り引き者が使用する装置に送信し、当該第３の要求に応じて前記第２の取り引き者から所定の応答を受けると、前記取り引きの履歴を記憶し、前記取り引きの正当性を認証する第２の署名情報を前記第１の取り引き者に提供する。

【００５２】

第１３の発明の認証システムは、前記第１の認証装置は、暗号化手段をさらに有し、前記送受信手段は、前記第２の取り引き者との間の通信に用いる暗号鍵を前記第２の要求に応じて前記第２の認証装置から受信し、前記暗号化手段で前記暗号鍵を用いて暗号化された前記取り引き内容に関する情報と前記第１の署名情

報とを、前記第２の取り引き者が使用する装置に送信する。

【００５３】

第１４の発明の認証方法は、第１の取り引き者に関する取り引きを認証する第１の認証装置と、第２の取り引き者に関する取り引きを認証する第２の認証装置とを用いて、ネットワークを介して行われる前記第１の取り引き者と前記第２の取り引き者との間の取り引きに関する認証を行う認証方法であって、前記第１の取り引き者から前記第１の認証装置に、前記取り引き内容を示す情報と前記第２の取り引き者を特定する情報とを含む第１の要求を出し、前記第１の要求に応じて、前記第１の認証装置から前記第２の認証装置に、前記第２の取り引き者を特定する情報を含む第２の要求を送信し、前記第２の要求に応じて、前記第２の認証装置からの前記第１の認証装置に、当該第２の認証装置による認証結果を示す第１の署名情報を送信し、前記第１の認証装置から前記第２の取り引き者が使用する装置に、前記第１の要求に含まれる前記取り引き内容に関する情報と前記第１の署名情報とを含む第３の要求を送信し、当該第３の要求に応じて、前記第２の取り引き者が使用する装置から前記第１の認証装置に所定の応答を出し、前記所定の応答に応じて、前記第１の認証装置は、前記取り引きの履歴を記憶し、前記取り引きの正当性の認証結果を示す第２の署名情報を作成し、当該第２の署名情報を、前記第１の取り引き者が使用する装置に送信する。

【００５４】

第１５の発明の通信装置は、利用者を識別するための個人識別情報を含む要求を受信する受信手段と、前記個人識別情報と処理結果を送信する送信先の情報とを対応付けて記憶する記憶手段と、前記要求に応じて所定の処理を行う処理手段と、前記要求に含まれる前記個人識別情報に対応する前記送信先の情報を前記記憶手段から読み出し、当該読み出した前記送信先の情報によって特定された送信先に、前記処理の結果を送信する送信手段とを有する。

【００５５】

第１５の発明の通信装置の作用は以下のようになる。

例えば、利用者が他の通信装置を操作して、利用者を識別するための個人識別情報を含む要求を送信する。

当該要求は、受信手段で受信される。

次に、処理手段において、当該受信した要求に応じた所定の処理が行われる。

次に、送信手段によって、前記受信した要求に含まれる前記個人識別情報に対応する前記送信先の情報が記記憶手段から読み出され、当該読み出された前記送信先の情報によって特定された送信先に、前記処理の結果が送信される。

【００５６】

第１５の発明の通信装置は、好ましくは、前記受信手段は、暗号化された前記個人識別情報を含む前記要求を受信し、前記通信装置は、前記受信した要求に含まれる前記個人識別情報を復号する復号手段をさらに有する。

また、第１５の発明の通信装置は、好ましくは、前記個人識別情報は、当該通信装置に登録された利用者に予め割り当てられた識別子である。

また、第１５の発明の通信装置は、好ましくは、前記処理の結果を送信する送信先の情報は、前記要求の送信元がオフラインで当該通信装置に提供した情報である。

また、第１５の発明の通信装置は、好ましくは、前記所定の結果を送信する送信先の情報は、当該通信装置が接続されるネットワークにおいて、前記利用者を一意に識別するための個人識別情報である。

また、第１５の発明の通信装置は、好ましくは、前記処理は、認証処理である。

【００５７】

第１６の発明の通信システムは、ネットワークを介して接続される第１の通信装置および第２の通信装置を有する通信システムであって、前記第１の通信装置は、利用者を識別するための個人識別情報を含む要求を受信する第１の受信手段と、前記個人識別情報と処理の結果を送信する送信先の情報とを対応付けて記憶する記憶手段と、前記要求に応じて所定の処理を行う処理手段と、前記要求に含まれる前記個人識別情報に対応する前記送信先の情報を前記記憶手段から読み出し、当該読み出した前記送信先の情報によって特定された送信先に、前記処理の結果を送信する第１の送信手段とを有し、前記第２の通信装置は、前記要求を前記第１の通信装置に送信する第２の送信手段と、前記処理の結果を前記第１の通

信装置から受信する第２の受信手段と、当該受信した認証処理の結果を出力する出力手段とを有する。

【００５８】

第１７の発明の通信方法は、ネットワークを介して接続される第１の通信装置および第２の通信装置を用いた通信方法であって、利用者を識別するための個人識別情報を含む要求を、前記第２の通信装置から前記第１の通信装置に送信し、前記第１の通信装置において、前記要求に応じて所定の処理を行い、前記第１の通信装置は、予め用意された前記個人識別情報と処理の結果を送信する送信先の情報とを対応関係を参照し、前記要求に含まれる前記個人識別情報に対応する送信先の情報によって特定される送信先に、前記処理の結果を送信する。

【００５９】

第１８の発明の通信制御装置は、単数または複数の第１の通信装置からの要求に応じてネットワーク上の第２の通信装置で処理を行うことに関しての通信を制御する通信制御装置であって、前記第１の通信装置を識別するための装置識別情報を記憶する記憶手段と、前記第１の通信装置からの要求に応じて、当該第１の通信装置に対応する前記装置識別情報を含む要求を前記第２の通信装置に送信する送信手段と、前記要求の送信元の装置を識別するための装置識別情報を含む応答を前記第２の通信装置から受信する受信手段と、前記応答に含まれる前記装置識別情報と前記記憶手段に記憶された前記装置識別情報とが一致するか否かに基づいて、前記受信した応答に対応した前記要求が、前記記憶手段に前記装置識別情報が記憶されている正当な前記第１の通信装置によるものであるかを判断する制御手段とを有する。

【００６０】

第１８の発明の通信制御装置の作用は以下のようになる。

送信手段、第１の通信装置からの要求に応じて、当該第１の通信装置に対応する前記装置識別情報を含む要求を第２の通信装置に送信する。

そして、受信手段が、前記要求の送信元の装置を識別するための装置識別情報を含む応答を前記第２の通信装置から受信する。

次に、制御手段によって、前記受信した応答に含まれる前記装置識別情報と記

憶手段に記憶された前記装置識別情報とが一致するか否かに基づいて、前記受信した応答に対応した前記要求が、前記記憶手段に前記装置識別情報が記憶されている正当な前記第１の通信装置によるものであるかを判断する。

【００６１】

第１８の発明の通信制御装置は、好ましくは、前記制御手段は、前記応答に含まれる前記装置識別情報と前記記憶手段に記憶された前記装置識別情報とが一致しない場合に、前記第２の通信装置に所定の通知を行う。

第１８の発明の通信制御装置は、好ましくは、前記制御手段は、前記応答に含まれる装置識別情報と前記記憶手段に記憶された前記装置識別情報とが一致しない場合に、前記応答に含まれる処理の結果が用いられる取り引き先の装置に所定の通知を行う。

また、第１８の発明の通信制御装置は、好ましくは、前記送信手段は、前記第１の通信装置から受信した個人識別情報と、当該第１の通信装置に対応する前記装置識別情報とを含む前記要求を前記第２の通信装置に送信する。

また、第１８の発明の通信制御装置は、好ましくは、前記記憶手段は、前記第１の通信装置から受信した前記装置識別情報を記憶する。

【００６２】

また、第１８の発明の通信制御装置は、好ましくは、前記記憶手段は、当該通信制御装置の電源が投入されたときに前記第１の通信装置から受信した前記装置識別情報を記憶する。

また、第１８の発明の通信制御装置は、好ましくは、前記制御手段は、前記第１の通信装置と前記第２の通信装置との間の通信履歴を前記記憶手段に書き込む。

また、第１８の発明の通信制御装置は、好ましくは、前記制御手段は、前記応答に含まれる前記第２の通信装置の処理結果を、前記要求の送信元の前記第１の通信装置に送信する。

また、第１８の発明の通信制御装置は、好ましくは、前記制御手段は、前記受信手段から受信した情報に応じて、待機状態にある前記第１の通信装置が動作状態になるように制御する。

また、第１８の発明の通信制御装置は、好ましくは、前記制御手段は、前記第１の通信装置が接続されたネットワークと、前記第２の通信装置が接続されたネットワークとの間の通信を制御する。

また、第１８の発明の通信制御装置は、好ましくは、前記装置識別情報は、前記第１の通信装置の製造元で付された当該通信装置を一意に識別可能な識別子である。

また、第１８の発明の通信制御装置は、好ましくは、前記個人識別情報は、登録した利用者に予め割り当てられた識別子である。

【００６３】

第１９の発明の通信システムは、単数または複数の第１の通信装置からの要求に応じてネットワーク上の第２の通信装置で処理を行うことに関する通信を通信制御装置で制御する通信システムであって、前記通信制御装置は、前記第１の通信装置を識別するための装置識別情報を記憶する第１の記憶手段と、前記第１の通信装置からの要求に応じて、当該第１の通信装置に対応する前記装置識別情報と個人識別情報とを含む要求を前記第２の通信装置に送信する第１の送信手段と、前記要求の送信元の装置を識別するための装置識別情報を含む応答を前記第２の通信装置から受信する第１の受信手段と、前記応答に含まれる前記装置識別情報と前記第１の記憶手段に記憶された前記装置識別情報とが一致するか否かに基づいて、前記受信した応答に対応した前記要求が、前記第１の記憶手段に前記装置識別情報が記憶されている正当な前記第１の通信装置によるものであるかを判断する制御手段とを有し、前記第２の通信装置は、前記要求を受信する第２の受信手段と、前記個人識別情報と処理結果を送信する送信先の情報とを対応付けて記憶する第２の記憶手段と、前記要求に応じて所定の処理を行う処理手段と、前記要求に含まれる前記個人識別情報に対応する前記送信先の情報を前記第２の記憶手段から読み出し、当該読み出した前記送信先の情報によって特定された送信先に、前記処理の結果と前記要求に含まれる前記装置識別情報とを対応付けて送信する第２の送信手段とを有する。

【００６４】

第２０の発明の通信方法は、単数または複数の第１の通信装置からの要求に応

じてネットワーク上の第２の通信装置で処理を行うことに関する通信を通信制御装置で制御する通信方法であって、前記第１の通信装置から前記通信制御装置に出された要求に応じて、当該第１の通信装置に対応する装置識別情報と個人識別情報とを含む要求を前記通信制御装置から前記第２の通信装置に送信し、前記第２の通信装置において、受信した前記要求に応じた所定の処理を行い、前記第２の通信装置において、前記要求に含まれる前記個人識別情報に対応する送信先の情報に基づいて、前記処理の結果と前記要求に含まれる前記装置識別情報とを含む応答を前記通信制御装置に送信し、前記通信制御装置において、受信した前記応答に含まれる前記装置識別情報と、予め保持した前記第１の通信装置の前記装置識別情報とが一致するか否かに基づいて、前記受信した応答に対応した前記要求が、正当な前記第１の通信装置によるものであるかを判断する。

【００６５】

第２１の発明の情報記録方法は、それぞれ単独では所定の情報の秘匿性が保持される複数のモジュールに前記所定の情報を分割し、前記複数のモジュールを相互に異なる記録媒体または同一の記録媒体の異なる領域に記録する。

【００６６】

第２１の発明の情報記録方法は、好ましくは、前記複数のモジュールが記録される相互に異なる複数の記録媒体は、物理的に相互に独立している記録媒体である。

また、第２１の発明の情報記録方法は、好ましくは、前記所定の情報を暗号化し、当該暗号化によって得た情報を、それぞれ単独では所定の情報の秘匿性が保持される前記複数のモジュールに分割する。

また、第２１の発明の情報記録方法は、好ましくは、前記複数のモジュールをそれぞれ暗号化し、当該暗号化によって得られた複数のモジュールを相互に異なる記録媒体または同一の記録媒体の異なる領域に記録する。

【００６７】

第２２の発明の情報復元方法は、それぞれ単独では所定の情報の秘匿性が保持される複数のモジュールが相互に異なる複数の記録媒体または同一の記録媒体の異なる領域に記録されている場合に、前記複数の記録媒体または同一の記録媒体

の異なる領域からそれぞれ前記モジュールを読み出し、当該読み出したモジュールを合成して前記所定の情報を復元する。

【００６８】

第２２の発明の情報復元方法は、好ましくは、前記複数のモジュールが記録される相互に異なる複数の記録媒体は、物理的に相互に独立している記録媒体である。

また、第２２の発明の情報復元方法は、好ましくは、前記読み出したモジュールを合成した後に復号して前記所定の情報を復元する。

また、第２２の発明の情報復元方法は、好ましくは、前記読み出したモジュールを復号した後に合成して前記所定の情報を復元する。

【００６９】

第２３の発明の情報記録装置は、それぞれ単独では所定の情報の秘匿性が保持される複数のモジュールに前記所定の情報を分割する情報分割手段と、前記複数のモジュールを相互に異なる記録媒体または同一の記録媒体の異なる領域に書き込む書き込み手段とを有する。

【００７０】

第２４の発明の情報復元装置は、それぞれ単独では所定の情報の秘匿性が保持される複数のモジュールが相互に異なる複数の記録媒体または同一の記録媒体の異なる領域に記録されている場合に、前記複数の記録媒体または同一の記録媒体の異なる領域からそれぞれ前記モジュールを読み出す読み出し手段と当該読み出したモジュールを合成して前記所定の情報を復元する情報合成手段とを有する。

【００７１】

第２５の発明の記録媒体は、それぞれ単独では所定の情報の秘匿性が保持される複数のモジュールに前記所定の情報を分割した場合に、前記複数のモジュールのうち一のモジュールが記録されている。

【００７２】

第２６の発明の認証方法は、認証装置において、ユーザの認証情報を第１の認証情報および第２の認証情報に分割し、前記第２の認証情報を記憶した携帯型メモリ装置を前記ユーザに提供し、前記携帯型メモリ装置にアクセス可能な端末装

置から前記認証装置に認証情報要求を送信し、前記認証装置において、前記認証情報要求が正当なユーザによるものであると判断した場合に、前記認証装置から前記端末装置に前記第１の認証情報を送信し、前記端末装置において、前記認証装置から受信した前記第１の認証情報と、前記携帯型メモリ装置から読み出した前記第２の認証情報とを用いて前記認証情報を復元する。

【００７３】

第２６の発明の認証方法によれば、ユーザの個人を認証する認証情報のうち一部の第２の認証情報のみを携帯型メモリ装置に記憶することから、ユーザが携帯型メモリ装置を盗まれたり、落としたりした場合に、他人は、携帯型メモリ装置のみでは、不正な認証処理を行うことができない。このとき、認証情報の全体を得るには、認証装置において正当なユーザであるかの確認を行う必要がある。

【００７４】

第２６の発明の認証方法は、好ましくは、前記認証情報要求は、前記第１の認証情報の送信先を指定した送信先情報を含み、前記認証装置は、前記送信先情報で指定された前記端末装置に、前記第１の認証情報を送信する。

【００７５】

第２６の発明の認証方法は、好ましくは、前記認証装置は、前記ユーザに対応する送信先情報を予め記憶し、当該記憶した送信先情報内に、前記認証情報要求に含まれる前記送信先情報が存在する場合に、前記認証情報要求が正当なユーザによるものであると判断する。

【００７６】

第２６の発明の認証方法は、好ましくは、前記端末装置は、前記認証装置から受信した前記第１の認証情報と、前記携帯型メモリ装置から読み出した前記第２の認証情報とが対応していると判断した場合に、前記受信した第１の認証情報を記憶して前記認証情報を復元する。

【００７７】

第２６の発明の認証方法は、好ましくは、前記端末装置は、前記認証装置から受信した前記第１の認証情報と、前記携帯型メモリ装置から読み出した前記第２の認証情報とが対応していない場合に、その旨を示す通知を前記認証装置に送信

する。

【００７８】

第２６の発明の認証方法は、好ましくは、前記認証装置は、前記ユーザからの要求に応じて、前記認証情報を生成する。

【００７９】

第２６の発明の認証方法は、好ましくは、前記認証情報は、公開鍵暗号を用いて作成された情報である。

【００８０】

第２６の発明の認証方法は、好ましくは、前記携帯型メモリ装置は、スマートメディアである。

【００８１】

第２７の発明の認証方法は、認証情報を生成し、前記認証情報を第１の認証情報および第２に認証情報に分割し、前記第２の認証情報を記憶した携帯型メモリ装置をユーザに提供し、受信した認証情報要求が正当なユーザによるものであると判断した場合に、前記認証情報要求が指定する送信先に、前記第１の認証情報を送信する。

【００８２】

第２８の発明の認証装置は、認証情報を生成し、前記認証情報を第１の認証情報および第２に認証情報に分割し、受信した認証情報要求が正当なユーザによるものであるか否かを判断する制御手段と、携帯型メモリ装置に前記第２の認証情報を書き込む書込手段と、前記携帯型メモリ装置のユーザから前記認証情報要求を受信する受信手段と、前記認証情報要求が正当なユーザによるものであると判断された場合に、前記第１の認証情報を前記認証情報要求によって指定された送信先に送信する送信手段とを有する。

【００８３】

第２８の認証装置の作用は以下のようになる。

制御手段によって、ユーザの個人を認証するための認証情報が生成され、当該認証情報が第１の認証情報および第２に認証情報に分割される。

書込手段によって、携帯型メモリ装置に前記第２の認証情報が書き込まれる。

そして、受信手段が前記携帯型メモリ装置のユーザから認証情報要求を受信すると、制御手段によって、前記受信した認証情報要求が正当なユーザによるものであるか否かが判断される。

そして、前記認証情報要求が正当なユーザによるものであると判断された場合に、送信手段によって、前記第１の認証情報が前記認証情報要求によって指定された送信先に送信される。

【００８４】

【発明の実施の形態】

以下、本発明の実施形態に係わるトランザクション認証システムを図面を参照して説明する。

第１実施形態

図１は、本実施形態におけるトランザクション認証システム１０１の構成を示した構成図である。

トランザクション認証システム１０１は、発注者３１が発注処理を行う発注者端末装置１１１と、発注者３１の生体的特徴を利用して発注者３１が本人であることを認証する生体認証装置１２と、ネットワーク銀行（あるいはトランザクション認証局運営会社）１２１によって使用され、商取引情報の認証を行う認証装置１１３と、認証履歴を格納する認証履歴格納装置１４と、受注者３３が受注処理を行う受注者端末装置１１５とを有する。

本実施形態は、第４～７の発明に対応した実施形態であり、発注者端末装置１１１が本発明の第１の通信装置に対応し、認証装置１１３が本発明の認証装置に対応し、受注者端末装置１１５が本発明の第２の通信装置に対応している。また、発注者３１が本発明の第１の取り引き者に対応し、受注者３３が本発明の第２の取り引き者に対応している。

【００８５】

〔発注者端末装置１１１〕

図２は、発注者端末装置１１１の機能ブロック図である。

発注者端末装置１１１は、本システム利用の契約を行った一般利用者である発注者３１が使用する端末装置である。

発注者端末装置１１１は、図２に示すように、認証要求入力部１１１ａ、認証要求送信部１１１ｂ、認証応答受信部１１１ｃ、認証要求暗号化部１１１ｄおよび認証応答復号部１１１ｅを有する。

認証要求入力部１１１ａは、例えば、発注者３１によるキーボードなどの操作に応じて、発注情報ａ１および発注者個人キー情報ｋ１（本発明の第１の取り引き者の個人キー情報）の入力を行う。なお、本実施形態において、個人キー情報は、対応する者の課金に係わる情報である。

発注情報ａ１には、例えば、発注者３１の名前、住所、連絡先、受注者３３の個人ＩＤ情報ＩＤ２（本発明の第２の取り引き者の個人識別情報）および発注する商品またはサービスの内容が記述されている。

認証要求送信部１１１ｂは、認証要求入力部１１１ａに入力された発注情報ａ１および発注者個人キー情報を含む認証要求Ｉｎｆ１（本発明の第１の要求）を認証装置１１３に送信する。

認証応答受信部１１１ｃは、認証装置１１３から認証応答Ｉｎｆ４を受信する。

認証要求暗号化部１１１ｄは、認証要求Ｉｎｆ１を暗号化する。

認証応答復号部１１１ｅは、認証応答Ｉｎｆ４を復号する。

【００８６】

生体認証装置１２は、いわゆるバイオメトリックス（biometrics）を用いて利用者の個人認証を行う装置であり、具体的には、事前に取得し、生体認証装置１２に格納しておいた利用者（発注者３１）の指紋等の身体的特徴と、実際に認証を行おうとする利用者の指紋等とを比較し、その一致・不一致によって本人の認証を行う。なお、利用者本人の指紋等の情報を格納する生体認証装置１２の記録装置は、外部から電気的に切断されており、その情報が外部に流出しない構成となっている。

【００８７】

〔認証装置１１３〕

図３は、認証装置１１３の機能ブロック図である。

認証装置１１３は、本システムを運営するネットワーク銀行１２１が使用する

装置である。

認証装置１１３は、図３に示すように、認証要求受信部１１３ａ、発注者認証部１１３ｂ、要求生成部１１３ｃ、要求送信部１１３ｄ、応答受信部１１３ｅ、受注者認証部１１３ｆ、認証応答生成部１１３ｇ、認証応答暗号化部１１３ｈ、認証応答送信部１１３ｉ、要求暗号化部１１３ｊ、応答復号部１１３ｋおよび認証要求復号部１１３ｌを有する。

【００８８】

ここで、認証要求受信部１１３ａが本発明の第１の受信手段に対応し、発注者認証部１１３ｂおよび要求生成部１１３ｃが本発明の第１の認証手段に対応し、要求送信部１１３ｄが本発明の第１の送信手段に対応し、応答受信部１１３ｅが本発明の第２の受信手段に対応し、受注者認証部１１３ｆおよび認証応答生成部１１３ｇが本発明の第２の認証手段に対応し、認証応答暗号化部１１３ｈが本発明の暗号化手段に対応し、認証応答送信部１１３ｉが本発明の第２の送信手段に対応し、要求暗号化部１１３ｊが本発明の暗号化手段に対応し、応答復号部１１３ｋが本発明の復号手段に対応し、認証要求復号部１１３ｌが本発明の復号手段に対応している。

【００８９】

認証要求受信部１１３ａは、発注者端末装置１１１が送信した認証要求Ｉｎｆ１を受信する。

発注者認証部１１３ｂは、認証要求Ｉｎｆ１が含む発注者個人キー情報ｋ１を用いて発注者３１の認証を行い、認証情報Ａｕ１（本発明の第１の認証情報）を生成する。

要求生成部１１３ｃは、認証要求Ｉｎｆ１から個人キー情報ｋ１を削除して情報Ｉｎｆ１ａを生成し、当該情報Ｉｎｆ１ａと認証情報Ａｕ１とを含む要求Ｉｎｆ２（本発明の第２の要求）を生成する。

要求送信部１１３ｄは、要求Ｉｎｆ２を受注者端末装置１１５に送信する。

応答受信部１１３ｅは、受注者端末装置１１５から応答Ｉｎｆ３（本発明の応答）を受信する。

受注者認証部１１３ｆは、応答Ｉｎｆ３に含まれる受注者３３の個人ＩＤ情報

ＩＤ２および個人キー情報ｋ２を用いて受注者３３の認証を行い、認証情報Ａｕ２（本発明の第２の識別情報）を生成する。

【００９０】

認証応答生成部１１３ｇは、応答Ｉｎｆ３に認証情報Ａｕ２を付加して認証応答Ｉｎｆ４を生成する。

認証応答暗号化部１１３ｈは、認証応答Ｉｎｆ４を暗号化する。

認証応答送信部１１３ｉは、暗号化された認証応答Ｉｎｆ４を発注者端末装置１１１に送信する。

要求暗号化部１１３ｊは、要求生成部１１３ｃが生成した要求Ｉｎｆ２を暗号化する。

応答復号部１１３ｋは、応答Ｉｎｆ３を復号する。

認証要求復号部１１３１は、認証要求Ｉｎｆ１を復号する。

【００９１】

〔受注者端末装置１１５〕

図４は、受注者端末装置１１５の機能ブロック図である。

受注者端末装置１１５は、本システム利用の契約を行った商品販売業者等である商品の受注者３３が使用する。

受注者端末装置１１５は、要求受信部１１５ａ、要求復号部１１５ｂ、応答入力部１１５ｃ、応答生成部１１５ｄ、応答暗号化部１１５ｅおよび応答送信部１１５ｆを有する。

要求受信部１１５ａは、認証装置１１３から要求Ｉｎｆ２を受信する。

要求復号部１１５ｂは、要求Ｉｎｆ２を復号する。

応答入力部１１５ｃは、ユーザによる操作に応じて、受注確認情報Ｃ１および受注者３３の個人キー情報Ｚを入力する。

応答生成部１１５ｄは、要求Ｉｎｆ２、受注確認情報Ｃ１および受注者３３の個人キー情報Ｚを含む応答Ｉｎｆ３を生成する。

応答暗号化部１１５ｅは、応答Ｉｎｆ３を暗号化する。

応答送信部１１５ｆは、暗号化された応答Ｉｎｆ３を認証装置１１３に送信する。

【００９２】

本実施形態のトランザクション認証システム１０１では、電子商取引の当事者である発注者３１と受注者３３との間に、その商取引の第三者であるネットワーク銀行１２１（あるいはトランザクション認証局）が介在し、ネットワーク銀行１２１が当事者間で行われる電子商取引を認証装置１１３を用いて認証することにより電子商取引上の不正を防止する。トランザクション認証システム１０１の利用を希望する商取引当事者は、まず、このネットワーク銀行１２１との間で認証装置１３の利用契約を結ぶ。

【００９３】

例えば、図１に示すように、発注者３１は、インターネット、郵便等を用い、ネットワーク銀行（トランザクション認証局運営会社）２１に対して、契約に必要な情報の送付を行う。ここで送付する情報としては、発注者３１の氏名、住所等の他、代金等の落とし先となる発注者３１が契約している引き落とし銀行４２の銀行口座等があげられる。これらの情報を受け取ったネットワーク銀行１２１は、契約を行った発注者３１に対し、銀行４２からの代金引き落としの際にその正当性を証明する個人ＩＤ情報、および本システムにおいて発注者３１を識別するための個人キー情報の発行を行う。ここで発行された個人ＩＤ情報は銀行４２に対しても送られ、銀行４２は、商品等の代金引き落としの際にこの個人ＩＤ情報を認証し、代金の不正引き落としを防止する。

【００９４】

なお、図１では、発注者３１が利用契約を結ぶ場合についてのみ説明したが、商品販売業者等である商品の受注者３３も同様な手順によりネットワーク銀行１２１との利用契約を結ぶ。また、ここでは、個人ＩＤ情報と個人キー情報を別個に発行することとしたが、個人キー情報を個人ＩＤ情報としても利用できることとし、別個の個人ＩＤ情報を発行しない形態としてもよい。

【００９５】

次に、トランザクション認証システム１０１の動作について説明する。

ステップＳＴ１１：

電子商取引によって商品を購入しようとする発注者３１は、まず、インターネ

ットの商取引サイト等から商品に関する情報を入手し、購入を希望する商品の選択を行う。

購入する商品の選択を行った発注者３１は、次に、発注者３１が所有する図２に示す発注者端末装置１１１を用いて、選択した商品の発注処理を行う。

発注処理は、認証要求入力部１１１ａを用い、購入を希望する商品・数量等を指定する発注情報ａ１および発注者３１の個人キー情報である発注者個人キー情報ｋ１を入力することにより行う。ここで、発注者個人キー情報ｋ１の入力は、発注処理を行うたびに発注者３１が手動で行うこととしてもよいし、発注処理時、自動的に入力されることとしてもよい。

【００９６】

これにより、入力された発注情報ａ１および発注者個人キー情報ｋ１を含む認証要求Ｉｎｆ１が生成され、当該認証要求Ｉｎｆ１が認証要求暗号化部１１１ｄで暗号化された後、認証要求送信部１１１ｂを介して認証装置１１３に送信される。

このとき、認証要求送信部１１１ｂは、第三者による不正発注、児童のいたずら等による誤発注を防止するため、認証要求Ｉｎｆ１の送信を禁止する不正送信防止機能を有しており、この状態では認証要求Ｉｎｆ１の送信は行われない。

そのため、電子商取引を行おうとする発注者３１は、生体認証装置１２を用い、自己の認証を行い、この不正送信防止機能の解除を行う必要がある。

例えば、生体認証装置１２が発注者３１の指紋によって発注者３１を認証するものであった場合、発注者３１は、生体認証装置１２に自己の指紋を読み取らせ、発注者３１の指紋を読み取った生体認証装置１２は、読み取った指紋と、事前に取得し、内部に格納しておいた発注者３１本人の指紋データとを照合し、読み取った指紋が発注者３１本人のものであるか否か判断する。

そして、読み取った指紋が発注者３１本人のものであると判断された場合、生体認証装置１２は、認証が成立した旨の情報を認証要求送信部１１１ｂに指示を与え、この情報を受けた認証要求送信部１１１ｂは、不正送信防止機能を解除し、送られた認証要求をトランザクション認証局３２所有の認証装置１１３に送信する。

【００９７】

ステップＳＴ１２：

図３に示す認証装置１１３に送信された認証要求Ｉｎｆ１は、認証要求受信部１１３ａで受信され、認証要求復号部１１３１によって復号された後、発注者認証部１１３ｂに送られる。

次に、発注者認証部１１３ｂにおいて、認証要求Ｉｎｆ１に含まれる発注者個人キー情報ｋ１と、図示していない記録装置に格納された契約者の個人キー情報とを用いて正当な発注者３１であるか否かが判断される。

そして、正当な発注者３１であると判断されると、認証要求Ｉｎｆ１は要求生成部１１３ｃに送られて、要求生成部１１３ｃにおいて、認証要求Ｉｎｆ１から個人キー情報ｋ１を削除して生成された情報Ｉｎｆ１ａと、認証情報Ａｕ１とを含む要求Ｉｎｆ２（本発明の第２の要求）が生成される。

当該Ｉｎｆ２は、要求暗号化部１１３ｊにおいて暗号化された後に、要求送信部１１３ｄを介して受注者端末装置１１５に送信される。

また、認証要求Ｉｎｆ１は、認証履歴格納装置１４に認証履歴として記憶される。

【００９８】

ステップＳＴ１３：

受注者端末装置１１５に送信された要求Ｉｎｆ２は、要求受信部１１５ａによって受信された後、要求復号部１１５ｂにより復号され、受注者３３は、復号された要求Ｉｎｆ２に基づいて商品の受注処理を行う。

受注処理は、受注者３３が応答入力部１１５ｃを用い、受注確認情報Ｃ１および受注者３３の個人キー情報Ｚ（本発明の第２の取り引き者の個人キー情報）を入力することにより行われる。ここで、受注者個人キー情報Ｚの入力は、受注処理を行うたびに受注者３３が手動で行うこととしてもよいし、発送処理時、自動的に入力されることとしてもよい。

【００９９】

次に、応答生成部１１５ｄにおいて、要求Ｉｎｆ２、受注確認情報Ｃ１および受注者３３の個人キー情報Ｚを含む応答Ｉｎｆ３が生成され、当該応答Ｉｎｆ３

が、応答暗号化部１１５ｅで暗号化された後に、応答送信部１１５ｆを介して認証装置１１３に送信される。

【０１００】

ステップＳＴ１４：

認証装置１１３に送信された応答Ｉｎｆ３は、図３に示す応答受信部１１３ｅで受信され、応答復号部１１３ｋによって復号された後、受注者認証部１１３ｆに送られる。

次に、受注者認証部１１３ｆにおいて、応答Ｉｎｆ３に含まれる受注者個人キー情報Ｚと、図示していない記録装置に格納された契約者の個人キー情報とを用いて正当な受注者３３であるか否かが判断される。

そして、正当な受注者３３であると判断されると、応答Ｉｎｆ３は認証応答生成部１１３ｇに送られて、認証応答生成部１１３ｇにおいて、応答Ｉｎｆ３と、認証が成立したことを示す認証情報Ａｕ２とを含む認証応答Ｉｎｆ４が生成される。

当該認証応答Ｉｎｆ４は、認証応答暗号化部１１３ｈにおいて暗号化された後に、認証応答送信部１１３ｉを介して発注者端末装置１１１に送信される。

また、応答Ｉｎｆ３は、認証履歴格納装置１４に認証履歴として記憶される。

【０１０１】

発注者端末装置１１１に送信された認証応答Ｉｎｆ４は、図２に示す認証応答受信部１１１ｃで受信された後、認証応答復号手投１１ｅによって復号され、発注者３１は、この復号された認証応答Ｉｎｆ４を確認することにより、自己の商品発注が適正に受領された旨を知ることが可能となる。

その後、ネットワーク銀行２１は、発注者３１の個人キー情報ｋ１を用いて、発注者３１が契約する引き落とし銀行４２の銀行口座から、当該取り引きに伴う金額を引き落とす。当該引き落としは、ネットワーク銀行２１の銀行口座に引き落としてから受注者３３の銀行口座に振り込んでもよいし、発注者３１の銀行口座から受注者３３の銀行口座に振り込みを直接行ってもよい。

また、受注者３３は、発注情報ａ１に基づいて、発注者３１に商品およびサービスを提供する。

【０１０２】

以上説明したように、トランザクション認証システム１０１によれば、発注者端末装置１１１および受注者端末装置１１５を用いた、発注者３１と受注者３３との間の電子商取引を認証装置１１３を用いて認証することで、電子商取引の信頼性を高めることができる。

また、トランザクション認証システム１０１によれば、認証装置１１３から受注者端末装置１１５に送信される要求Ｉｎｆ２には、受注者３３の個人キー情報ｋ１を含まないため、発注者３１の課金に係わる個人キー情報が受注者３３に渡ることはない。そのため、個人キー情報の不正利用を効果的に抑制できる。

また、トランザクション認証システム１０１によれば、第三者が発注者個人キー情報ｋ１を盗用して偽発注を行った場合或いは情報の改竄を行った場合であっても、その発注に対する認証応答Ｉｎｆ４は正規の発注者３１に送信されることとなり、正規の発注者３１は、第三者による偽発注或いは改竄があったことを知ることができ、これにより電子取引上の不正を有効に防止することが可能となる。

【０１０３】

また、認証装置１１３によって、認証要求Ｉｎｆ１および応答Ｉｎｆ３を認証することとしたため、電子商取引においてやりとりされる情報の信頼性が増し、電子取引上の不正を有効に防止することが可能となる。

【０１０４】

さらに、認証履歴格納装置１４によって、認証要求Ｉｎｆ１および応答Ｉｎｆ３を格納することとしたため、電子商取引の履歴を第三者が客観的に証明することが可能となり、これにより電子商取引の当事者間で行われる不正を有効に防止することが可能となる。

【０１０５】

また、認証要求Ｉｎｆ１、要求Ｉｎｆ２、応答Ｉｎｆ３および認証応答Ｉｎｆ４は、暗号化されて送信されることとしたため、第三者による情報の改竄、盗用等を有効に防止することが可能となる。

【０１０６】

さらに、認証要求送信部１１１ｂは、生体認証装置１２によって発注者３１が本人であることが認証された場合にのみ、認証要求の送信を行うこととしたため、第三者による不正発注、児童のいたずら等による誤発注を防止することが可能となる。

【０１０７】

第２実施形態

図６は、本実施形態におけるトランザクション認証システム１の構成を示した構成図である。

トランザクション認証システム１は、発注者３１が発注処理を行う発注者端末装置１１と、発注者３１の生体的特徴を利用して発注者３１が本人であることを認証する生体認証装置１２と、ネットワーク銀行（あるいはトランザクション認証局運営会社）２１によって使用され、商取引情報の認証を行う認証装置１３と、認証履歴を格納する認証履歴格納装置１４と、受注者３３が受注処理を行う受注者端末装置１５とを有する。

本実施形態は、第１～３の発明に対応した実施形態であり、発注者端末装置１１が本発明の第１の通信装置に対応し、認証装置１３が本発明の認証装置に対応し、受注者端末装置１５が本発明の第２の通信装置に対応している。また、発注者３１が本発明の第１の取り引き者に対応し、受注者３３が本発明の第２の取り引き者に対応している。

【０１０８】

〔発注者端末装置１１〕

図７は、発注者端末装置１１の機能ブロック図である。

発注者端末装置１１は、本システム利用の契約を行った一般利用者である発注者３１が使用する端末装置である。

発注者端末装置１１は、図７に示すように、認証要求入力部１１ａ、認証要求送信部１１ｂ、認証応答受信部１１ｃ、認証要求暗号化部１１ｄおよび認証応答復号部１１ｅを有する。

認証要求入力部１１ａは、例えば、発注者３１によるキーボードなどの操作に応じて、発注情報ａ１、発注者個人ＩＤ情報ＩＤ１（本発明の第１の取り引き者

の個人識別情報）および発注者個人キー情報ｋ１（本発明の第１の取り引き者の個人キー情報）の入力を行う。なお、本実施形態において、個人キー情報は、対応する者の課金に係わる情報である。

発注情報ａ１には、例えば、発注者３１の名前、住所、連絡先、受注者３３の個人ＩＤ情報ＩＤ２（本発明の第２の取り引き者の個人識別情報）および発注する商品またはサービスの内容が記述されている。

認証要求送信部１１ｂは、認証要求入力部１１ａに入力された発注情報ａ１、発注者個人ＩＤ情報ＩＤ１および発注者個人キー情報を含む認証要求Ｉｎｆ１（本発明の第１の要求）を認証装置１３に送信する。

認証応答受信部１１ｃは、認証装置１３から認証応答Ｉｎｆ４を受信する。

認証要求暗号化部１１ｄは、認証要求Ｉｎｆ１を暗号化する。

認証応答復号部１１ｅは、認証応答Ｉｎｆ４を復号する。

【０１０９】

生体認証装置１２は、いわゆるバイオメトリックス（biometrics）を用いて利用者の個人認証を行う装置であり、具体的には、事前に取得し、生体認証装置１２に格納しておいた利用者（発注者３１）の指紋等の身体的特徴と、実際に認証を行おうとする利用者の指紋等とを比較し、その一致・不一致によって本人の認証を行う。なお、利用者本人の指紋等の情報を格納する生体認証装置１２の記録装置は、外部から電気的に切断されており、その情報が外部に流出しない構成となっている。

【０１１０】

〔認証装置１３〕

図８は、認証装置１３の機能ブロック図である。

認証装置１３は、本システムを運営するネットワーク銀行２１が使用する装置である。

認証装置１３は、図８に示すように、認証要求受信部１３ａ、発注者認証部１３ｂ、要求生成部１３ｃ、要求送信部１３ｄ、応答受信部１３ｅ、受注者認証部１３ｆ、認証応答生成部１３ｇ、認証応答暗号化部１３ｈ、認証応答送信部１３ｉ、要求暗号化部１３ｊ、応答復号部１３ｋおよび認証要求復号部１３１を有す

る。

【０１１１】

ここで、認証要求受信部１３ａが本発明の第１の受信手段に対応し、発注者認証部１３ｂおよび要求生成部１３ｃが本発明の第１の認証手段に対応し、要求送信部１３ｄが本発明の第１の送信手段に対応し、応答受信部１３ｅが本発明の第２の受信手段に対応し、受注者認証部１３ｆおよび認証応答生成部１３ｇが本発明の第２の認証手段に対応し、認証応答暗号化部１３ｈが本発明の暗号化手段に対応し、認証応答送信部１３ｉが本発明の第２の送信手段に対応し、要求暗号化部１３ｊが本発明の暗号化手段に対応し、応答復号部１３ｋが本発明の復号手段に対応し、認証要求復号部１３１が本発明の復号手段に対応している。

【０１１２】

認証要求受信部１３ａは、発注者端末装置１１が送信した認証要求Ｉｎｆ１を受信する。

発注者認証部１３ｂは、認証要求Ｉｎｆ１が含む発注者個人ＩＤ情報ＩＤ１および発注者個人キー情報ｋ１を用いて発注者３１の認証を行い、認証情報Ａｕ１（本発明の第１の認証情報）を生成する。

要求生成部１３ｃは、発注者認証部１３ｂによって認証された認証要求Ｉｎｆ１に認証情報Ａｕ１を付加して要求Ｉｎｆ２（本発明の第２の要求）を生成する。

要求送信部１３ｄは、要求Ｉｎｆ２を受注者端末装置１５に送信する。

応答受信部１３ｅは、受注者端末装置１５から応答Ｉｎｆ３（本発明の応答）を受信する。

受注者認証部１３ｆは、応答Ｉｎｆ３に含まれる受注者３３の個人ＩＤ情報ＩＤ２および個人キー情報ｋ２を用いて受注者３３の認証を行い、認証情報Ａｕ２（本発明の第２の識別情報）を生成する。

【０１１３】

認証応答生成部１３ｇは、応答Ｉｎｆ３に認証情報Ａｕ２を付加して認証応答Ｉｎｆ４を生成する。

認証応答暗号化部１３ｈは、認証応答Ｉｎｆ４を暗号化する。

認証応答送信部１３ｉは、暗号化された認証応答Ｉｎｆ４を発注者端末装置１１に送信する。

要求暗号化部１３ｊは、要求生成部１３ｃが生成した要求Ｉｎｆ２を暗号化する。

応答復号部１３ｋは、応答Ｉｎｆ３を復号する。

認証要求復号部１３１は、認証要求Ｉｎｆ１を復号する。

【０１１４】

〔受注者端末装置１５〕

図９は、受注者端末装置１５の機能ブロック図である。

受注者端末装置１５は、本システム利用の契約を行った商品販売業者等である商品の受注者３３が使用する。

受注者端末装置１５は、要求受信部１５ａ、要求復号部１５ｂ、応答入力部１５ｃ、応答生成部１５ｄ、応答暗号化部１５ｅおよび応答送信部１５ｆを有する。

要求受信部１５ａは、認証装置１３から要求Ｉｎｆ２を受信する。

要求復号部１５ｂは、要求Ｉｎｆ２を復号する。

応答入力部１５ｃは、ユーザによる操作に応じて、受注確認情報Ｃ１および受注者３３の個人キー情報Ｚを入力する。

応答生成部１５ｄは、要求Ｉｎｆ２、受注確認情報Ｃ１および受注者３３の個人キー情報Ｚを含む応答Ｉｎｆ３を生成する。

応答暗号化部１５ｅは、応答Ｉｎｆ３を暗号化する。

応答送信部１５ｆは、暗号化された応答Ｉｎｆ３を認証装置１３に送信する。

【０１１５】

本実施形態のトランザクション認証システム１では、電子商取引の当事者である発注者３１と受注者３３との間に、その商取引の第三者であるネットワーク銀行２１（あるいはトランザクション認証局）が介在し、ネットワーク銀行２１が当事者間で行われる電子商取引を認証装置１３を用いて認証することにより電子商取引上の不正を防止する。トランザクション認証システム１の利用を希望する商取引当事者は、まず、このネットワーク銀行２１との間で認証装置１３の利用

契約を結ぶ。

【０１１６】

例えば、図６に示すように、発注者３１は、インターネット、郵便等を用い、ネットワーク銀行２１に対して、契約に必要な情報の送付を行う。ここで送付する情報としては、発注者３１の氏名、住所等の他、代金等の落とし先となる発注者３１が契約している引き落とし銀行４２の銀行口座等があげられる。これらの情報を受け取ったネットワーク銀行２１は、契約を行った発注者３１に対し、銀行４２からの代金引き落としの際にその正当性を証明する個人ＩＤ情報、および本システムにおいて発注者３１を識別するための個人キー情報の発行を行う。ここで発行された個人ＩＤ情報は銀行４２に対しても送られ、銀行４２は、商品等の代金引き落としの際にこの個人ＩＤ情報を認証し、代金の不正引き落としを防止する。

【０１１７】

なお、図６では、発注者３１が利用契約を結ぶ場合についてのみ説明したが、商品販売業者等である商品の受注者３３も同様な手順によりネットワーク銀行２１との利用契約を結ぶ。また、ここでは、個人ＩＤ情報と個人キー情報を別個に発行することとしたが、個人キー情報を個人ＩＤ情報としても利用できることとし、別個の個人ＩＤ情報を発行しない形態としてもよい。

【０１１８】

次に、トランザクション認証システム１の動作について説明する。

ステップＳＴ１：

電子商取引によって商品を購入しようとする発注者３１は、まず、インターネットの商取引サイト等から商品に関する情報を入手し、購入を希望する商品の選択を行う。

購入する商品の選択を行った発注者３１は、次に、発注者３１が所有する図７に示す発注者端末装置１１を用いて、選択した商品の発注処理を行う。

発注処理は、認証要求入力部１１ａを用い、購入を希望する商品・数量等を指定する発注情報ａ１、契約時に発行された発注者３１の個人ＩＤ情報である発注者個人ＩＤ情報ＩＤ１、および発注者の個人キー情報である発注者個人キー情報

ｋ１を入力することにより行う。ここで、発注者個人ＩＤ情報ＩＤ１および発注者個人キー情報ｋ１の入力は、発注処理を行うたびに発注者３１が手動で行うこととしてもよいし、発注処理時、自動的に入力されることとしてもよい。

【０１１９】

これにより、入力された発注情報ａ１、発注者個人ＩＤ情報ＩＤ１および発注者個人キー情報ｋ１を含む認証要求Ｉｎｆ１が生成され、当該認証要求Ｉｎｆ１が認証要求暗号化部１１ｄで暗号化された後、認証要求送信部１１ｂを介して認証装置１３に送信される。

このとき、認証要求送信部１１ｂは、第三者による不正発注、児童のいたずら等による誤発注を防止するため、認証要求Ｉｎｆ１の送信を禁止する不正送信防止機能を有しており、この状態では認証要求Ｉｎｆ１の送信は行われない。

そのため、電子商取引を行おうとする発注者３１は、生体認証装置１２を用い、自己の認証を行い、この不正送信防止機能の解除を行う必要がある。

例えば、生体認証装置１２が発注者３１の指紋によって発注者３１を認証するものであった場合、発注者３１は、生体認証装置１２に自己の指紋を読み取らせ、発注者３１の指紋を読み取った生体認証装置１２は、読み取った指紋と、事前に取得し、内部に格納しておいた発注者３１本人の指紋データとを照合し、読み取った指紋が発注者３１本人のものであるか否か判断する。

そして、読み取った指紋が発注者３１本人のものであると判断された場合、生体認証装置１２は、認証が成立した旨の情報を認証要求送信部１１ｂに指示を与え、この情報を受けた認証要求送信部１１ｂは、不正送信防止機能を解除し、送られた認証要求をネットワーク銀行２１所有の認証装置１３に送信する。

【０１２０】

ステップＳＴ２：

図８に示す認証装置１３に送信された認証要求Ｉｎｆ１は、認証要求受信部１３ａで受信され、認証要求復号部１３１によって復号された後、発注者認証部１３ｂに送られる。

次に、発注者認証部１３ｂにおいて、認証要求Ｉｎｆ１に含まれる発注者個人ＩＤ情報ＩＤ１と、発注者個人キー情報ｋ１と、図示していない記録装置に格納

された契約者の個人キー情報とを用いて正当な発注者３１であるか否かが判断される。

そして、正当な発注者３１であると判断されると、認証要求Ｉｎｆ１は要求生成部１３ｃに送られて、要求生成部１３ｃにおいて、認証要求Ｉｎｆ１と、認証が成立したことを示す認証情報Ａｕ１とを含む要求Ｉｎｆ２が生成される。

当該Ｉｎｆ２は、要求暗号化部１３ｊにおいて暗号化された後に、要求送信部１３ｄを介して受注者端末装置１５に送信される。

また、認証要求Ｉｎｆ１は、認証履歴格納装置１４に認証履歴として記憶される。

【０１２１】

ステップＳＴ３：

受注者端末装置１５に送信された要求Ｉｎｆ２は、要求受信部１５ａによって受信された後、要求復号部１５ｂにより復号され、受注者３３は、復号された要求Ｉｎｆ２に基づいて商品の受注処理を行う。

受注処理は、受注者３３が応答入力部１５ｃを用い、受注確認情報Ｃ１および受注者３３の個人キー情報Ｚ（本発明の第２の取り引き者の個人キー情報）を入力することにより行われる。ここで、受注者個人キー情報Ｚの入力は、受注処理を行うたびに受注者３３が手動で行うこととしてもよいし、発送処理時、自動的に入力されることとしてもよい。

【０１２２】

次に、応答生成部１５ｄにおいて、要求Ｉｎｆ２、受注確認情報Ｃ１および受注者３３の個人キー情報Ｚを含む応答Ｉｎｆ３が生成され、当該応答Ｉｎｆ３が、応答暗号化部１５ｅで暗号化された後に、応答送信部１５ｆを介して認証装置１３に送信される。

【０１２３】

ステップＳＴ４：

認証装置１３に送信された応答Ｉｎｆ３は、図８に示す応答受信部１３ｅで受信され、応答復号部１３ｋによって復号された後、受注者認証部１３ｆに送られる。

次に、受注者認証部１３ｆにおいて、応答Ｉｎｆ３に含まれる受注者個人キー情報Ｚと、図示していない記録装置に格納された契約者の個人キー情報とを用いて正当な受注者３３であるか否かが判断される。

そして、正当な受注者３３であると判断されると、応答Ｉｎｆ３は認証応答生成部１３ｇに送られて、認証応答生成部１３ｇにおいて、応答Ｉｎｆ３と、認証が成立したことを示す認証情報Ａｕ２とを含む認証応答Ｉｎｆ４が生成される。

当該認証応答Ｉｎｆ４は、認証応答暗号化部１３ｈにおいて暗号化された後に、認証応答送信部１３ｉを介して発注者端末装置１１に送信される。

また、応答Ｉｎｆ３は、認証履歴格納装置１４に認証履歴として記憶される。

【０１２４】

発注者端末装置１１に送信された認証応答Ｉｎｆ４は、図７に示す認証応答受信部１１ｃで受信された後、認証応答復号手投１１ｅによって復号され、発注者３１は、この復号された認証応答Ｉｎｆ４を確認することにより、自己の商品発注が適正に受領された旨を知ることが可能となる。その後、受注者３３は、発注者３１の発注者個人ＩＤ情報ＩＤ１を用い、発注者３１が契約している銀行から、発注を受けた商品代金の引き落としを行い、さらに、発注を受けた商品を発注者３１に郵送する。

【０１２５】

以上説明したように、トランザクション認証システム１によれば、発注者端末装置１１および受注者端末装置１５を用いた、発注者３１と受注者３３との間の電子商取引を認証装置１３を用いて認証することで、電子商取引の信頼性を高めることができる。

また、トランザクション認証システム１によれば、第三者が発注者個人キー情報ｋ１を盗用して偽発注を行った場合或いは情報の改竄を行った場合であっても、その発注に対する認証応答Ｉｎｆ４は正規の発注者３１に送信されることとなり、正規の発注者３１は、第三者による偽発注或いは改竄があったことを知ることができ、これにより電子取引上の不正を有効に防止することが可能となる。

【０１２６】

また、認証装置１３によって、認証要求Ｉｎｆ１および応答Ｉｎｆ３を認証す

ることとしたため、電子商取引においてやりとりされる情報の信頼性が増し、電子取引上の不正を有効に防止することが可能となる。

【０１２７】

さらに、認証履歴格納装置１４によって、認証要求Ｉｎｆ１および応答Ｉｎｆ３を格納することとしたため、電子商取引の履歴を第三者が客観的に証明することが可能となり、これにより電子商取引の当事者間で行われる不正を有効に防止することが可能となる。

【０１２８】

また、認証要求Ｉｎｆ１、要求Ｉｎｆ２、応答Ｉｎｆ３および認証応答Ｉｎｆ４は、暗号化されて送信されることとしたため、第三者による情報の改竄、盗用等を有効に防止することが可能となる。

【０１２９】

さらに、認証要求送信部１１ｂは、生体認証装置１２によって発注者３１が本人であることが認証された場合にのみ、認証要求の送信を行うこととしたため、第三者による不正発注、児童のいたずら等による誤発注を防止することが可能となる。

【０１３０】

なお、上記の処理機能は、コンピュータによって実現することができる。その場合、発注者端末装置１１、認証装置１３、受注者端末装置１５が有すべき機能の処理内容は、コンピュータで読み取り可能な記録媒体に記録されたプログラムに記述しておく。そして、このプログラムをコンピュータで実行することにより、上記処理がコンピュータで実現される。コンピュータで読み取り可能な記録媒体としては、磁気記録装置や半導体メモリ等がある。市場に流通させる場合には、ＣＤ－ＲＯＭ（Ｃｏｍｐａｃｔ　Ｄｉｓｃ　Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）やフロッピーディスク等の可搬型記録媒体にプログラムを格納して流通させたり、ネットワークを介して接続されたコンピュータの記憶装置に格納しておき、ネットワークを通じて他のコンピュータに転送することもできる。コンピュータで実行する際には、コンピュータ内のハードディスク装置等にプログラムを格納しておき、メインメモリにロードして実行する。

【０１３１】

なお、本形態では、トランザクション認証システム１を、電子商取引において利用することとしたが、電子通信回線を用いたアンケート、投票、その他情報伝送時における不正防止のために利用することとしてもよい。

【０１３２】

第３実施形態

図１１は、本実施形態のトランザクション認証システム３０１の全体構成図である。

図１１に示すように、トランザクション認証システム３０１では、例えば、発注者３１の発注者端末装置３１１と、受注者３３の受注者端末装置３１５と、ネットワーク銀行３４０の認証装置３５０と、ネットワーク銀行３４１の認証装置３５１と、認証履歴を格納する認証履歴格納装置１４とが、インターネットなどのネットワーク（通信網）を介して接続されており、発注者３１と受注者３３との間のトランザクション（取り引き）の正当性を認証する。

【０１３３】

本実施形態では、例えば、発注者３１とネットワーク銀行３４０との間で認証を行うことに関しての契約が成されており、受注者３３とネットワーク銀行３４１との間で認証を行うことに関しての契約が成されている。

また、ネットワーク銀行３４０とネットワーク銀行３４１とでは、認証に関して、相互に連携する旨の相互乗り入れの契約が成立されている。

【０１３４】

本実施形態は、第１２～１４の発明に対応した実施形態である。

本実施形態では、発注者３１が本発明の第１の取り引き者に対応し、受注者３３が本発明の第２の取り引き者に対応している。

また、認証装置３５０が、第１２の発明の認証装置、並びに第１３の発明および第１４の発明の第１の認証装置に対応している。

また、認証装置３５１が、第１２の発明の他の認証装置、並びに第１３の発明および第１４の発明の第２の認証装置に対応している。

【０１３５】

以下、トランザクション認証システム３０１を構成する各装置について説明する。

〔発注者端末装置３１１〕

図１２に示すように、発注者端末装置３１１は、例えば、発注者３１の家庭などに設けられた、パーソナルコンピュータ、セット・トップ・ボックスあるいはゲーム機器などの装置であり、受信部３６１、送信部３６２、暗号化部３６３、復号部３６４、記憶部３６５、制御部３６６および署名検証部３６７を有する。

なお、発注者端末装置３１１は、例えば、発注者３１が使用する際に、発注者３１の指紋等の身体的特徴から得られる情報と、予め記憶部３６５に予め記憶してある身体的特徴を示す情報とを比較することで、発注者３１が正当な使用者であることを認証する生態認証部を有していてもよい。

【０１３６】

受信部３６１は、ネットワークを介して認証装置３５０から情報あるいは要求を受信する。

送信部３６２は、ネットワークを介して認証装置３５０に情報あるいは要求を送信する。

また、受信部３６１および送信部３６２は、受注者３３が提供する商品等の案内情報にアクセスする際に、ネットワークを介して、当該サーバ装置との間で情報あるいは要求の送受信を行う。

暗号化部３６３は、所定の暗号鍵を用いて、情報あるいは要求を暗号化する。

復号部３６４は、所定の暗号鍵を用いて、情報あるいは要求を復号する。

記憶部３６５は、例えば、発注者３１がネットワーク銀行３４０と契約を行うと、例えば、発注者３１に割り当てられた秘密鍵$K_{31,S}$などを格納する。

制御部３６６は、発注者端末装置３１１内の各構成要素の処理を統括的に制御する。

署名検証部３６７は、例えば、認証装置３５０が作成した署名情報を、ネットワーク銀行３４０の公開鍵$K_{40,P}$を用いて検証する。

【０１３７】

〔受注者端末装置３１５〕

図１３に示すように、受注者端末装置３１５は、サイバーモール(Cyber Moll)などに店舗を出している受注者３３が使用するサーバ装置であり、受信部３７１、送信部３７２、暗号化部３７３、復号部３７４、記憶部３７５、制御部３７６および署名検証部３７７を有する。

受信部３７１は、ネットワークを介して認証装置３５０，３５１から情報あるいは要求を受信する。

送信部３７２は、ネットワークを介して認証装置３５０，３５１に情報あるいは要求を送信する。

また、受信部３７１および送信部３７２は、発注者端末装置３１１からのアクセスに応じて、例えば、記憶部３７５から読み出した受注者３３が提供する商品等の案内情報を、ネットワークを介して、発注者端末装置３１１に送信する。

暗号化部３７３は、所定の暗号鍵を用いて、情報あるいは要求を暗号化する。

復号部３７４は、所定の暗号鍵を用いて、情報あるいは要求を復号する。

記憶部３７５は、例えば、受注者３３がネットワーク銀行３４１と契約を行うと、例えば、受注者３３に割り当てられた秘密鍵$K_{33,S}$などを格納する。

制御部３７６は、受注者端末装置３１５内の各構成要素の処理を統括的に制御する。

署名検証部３７７は、例えば、受注者３３の公開鍵$K_{33,P}$を用いて、受注者端末装置３１５が作成した署名情報の検証を行う。

【０１３８】

〔認証装置３５０〕

図１４に示すように、認証装置３５０は、受信部３８１、送信部３８２、暗号化部３８３、復号部３８４、記憶部３８５、制御部３８６、署名作成部３８７および課金処理部３８８を有する。

ここで、受信部３８１および送信部３８２が、第１２の発明の送受信手段に対応し、記憶部３８５が第１２の発明の記憶手段に対応し、署名作成部３８７が第１２の発明の署名作成手段に対応している。

【０１３９】

受信部３８１は、ネットワークを介して発注者端末装置３１１、受注者端末装

置３１５および認証装置３５１から情報あるいは要求を受信する。

送信部３８２は、ネットワークを介して発注者端末装置３１１、受注者端末装置３１５および認証装置３５１に情報あるいは要求を送信する。

暗号化部３８３は、所定の暗号鍵を用いて、情報あるいは要求を暗号化する。

復号部３８４は、所定の暗号鍵を用いて、情報あるいは要求を復号する。

記憶部３８５は、例えば、発注者３１がネットワーク銀行３４０と契約を行うと、例えば、発注者３１に割り当てられた秘密鍵$K_{31,S}$に対応する公開鍵$K_{33,P}$などを格納する。

制御部３８６は、認証装置３５０内の各構成要素の処理を統括的に制御する。

署名作成部３８７は、ネットワーク銀行３４０の秘密鍵$K_{40,S}$を用いて署名情報の作成を行う。

課金処理部３８８は、発注者３１による取り引きに関する認証に対しての課金処理を行い、認証装置３５１との間で、前記取り引きに関する認証に対して行う課金の割合を決定するための処理を行う。

認証装置３５０の各構成要素の詳細な処理については、後述する動作例で記載する。

【０１４０】

図１５に示すように、認証装置３５１は、受信部３９１、送信部３９２、暗号化部３９３、復号部３９４、記憶部３９５、制御部３９６、署名作成部３９７および課金処理部３９８を有する。

受信部３９１は、ネットワークを介して受注者端末装置３１５および認証装置３５０から情報あるいは要求を受信する。

送信部３９２は、ネットワークを介して受注者端末装置３１５および認証装置３５０に情報あるいは要求を送信する。

暗号化部３９３は、所定の暗号鍵を用いて、情報あるいは要求を暗号化する。

復号部３９４は、所定の暗号鍵を用いて、情報あるいは要求を復号する。

記憶部３９５は、受注者３３がネットワーク銀行３４１と契約を行うと、例えば、受注者３３に割り当てられた秘密鍵$K_{33,S}$に対応する公開鍵$K_{33,P}$などを格

納する。

制御部３９６は、認証装置３５１内の各構成要素の処理を統括的に制御する。

署名作成部３９７は、ネットワーク銀行３４１の秘密鍵$K_{41,S}$を用いて署名情報の作成を行う。

課金処理部３９８は、受注者３３による取り引きに関する認証に対しての課金処理を行い、認証装置３５０との間で、前記取り引きに関する認証に対して行う課金の割合を決定するための処理を行う。

【０１４１】

以下、トランザクション認証システム３０１の動作例を説明する。

以下に示す動作例を開始する前提として、発注者３１とネットワーク銀行３４０との間で所定の契約が結ばれ、ネットワーク銀行３４０は、発注者３１に対して、個人キー情報ｋ１および個人ＩＤ情報ＩＤ１を発行する。ネットワーク銀行３４０は、個人キー情報ｋ１および個人ＩＤ情報ＩＤ１の対応表を図１４に示す認証装置３５０の記憶部３８５に記憶する。ここで、個人キー情報ｋ１は、例えば、ネットワーク銀行３４０と契約した契約者（発注者３１）の契約番号などの個人情報を示す識別子である。また、個人ＩＤ情報ＩＤ１は、発注者３１の銀行口座番号などの課金に係わる情報を示す識別子である。

また、ネットワーク銀行３４０は、自らの秘密鍵$K_{40,S}$を図１４に示す認証装置３５０の記憶部３８５に記憶すると共に、当該秘密鍵$K_{40,S}$に対応する公開鍵$K_{40,P}$を発注者端末装置３１１に送信する。発注者端末装置３１１は、公開鍵$K_{40,P}$を図１２に示す記憶部３６５に記憶する。

【０１４２】

また、受注者３３とネットワーク銀行３４１との間で所定の契約が結ばれ、ネットワーク銀行３４１は、受注者３３に対して、個人キー情報Ｚおよび個人ＩＤ情報ＩＤ２を発行する。ネットワーク銀行３４１は、個人キー情報Ｚおよび個人ＩＤ情報ＩＤ２の対応表を図１５に示す認証装置３５１の記憶部３９５に記憶する。

また、ネットワーク銀行３４１は、自らの秘密鍵$K_{41,S}$を図１５に示す認証装置３５１の記憶部３９５に記憶すると共に、当該秘密鍵$K_{41,S}$に対応する公開鍵

$K_{41,P}$を受注者端末装置３１５に送信する。受注者端末装置３１５は、公開鍵$K_{41,P}$を図１３に示す記憶部３７５に記憶する。

【０１４３】

また、ネットワーク銀行３４０とネットワーク銀行３４１との間では、認証に関して相互乗り入れの契約がなされている。なお、認証装置３５０と認証装置３５１との間では、当該契約に基づいて、要求および情報の伝送が、公開鍵暗号方式あるいは共通鍵暗号方式を用いて行われる。

【０１４４】

図１６は、トランザクション認証システム３０１の動作例を説明するための図である。

ステップＳＴ３１：

発注者端末装置３１１は、図１１に示す発注者３１は、例えばネットワーク上の商店である受注者３３に商品を発注する場合に、受注者３３を特定する情報（例えば受注者３３の名前）、発注する商品名および数量などを示す発注情報ａ１と、発注者３１の個人キー情報ｋ１と、発注者３１の個人ＩＤ情報ＩＤ１とを、図示しない操作手段を操作して発注者端末装置３１１に入力する。なお、発注情報ａ１には、受注者３３を特定する情報が含まれている。

次に、図１２に示す発注者端末装置３１１の暗号化部３６３は、記憶部３６５から読み出した所定の暗号鍵を用いて、発注情報ａ１と、個人キー情報ｋ１および個人ＩＤ情報ＩＤ１を暗号化し、当該暗号化した情報を格納した認証要求Ｉｎｆ１（本発明の第１の要求）を、送信部３６２からネットワークを介して、図１１に示すネットワーク銀行３４０に送信する。

【０１４５】

ステップＳＴ３２：

図１４に示す認証装置３５０は、発注者端末装置３１１からの認証要求Ｉｎｆ１を受信部３８１が受信すると、記憶部３８５から所定の暗号化鍵を読み出し、復号部３８４において、当該暗号鍵を用いて認証要求Ｉｎｆ１を復号する。

次に、認証装置３５０は、制御部３８６の制御に基づいて、上記復号した認証要求Ｉｎｆ１に格納された発注情報ａ１に含まれる受注者３３を特定する情報ｂ

１を格納した要求Ｉｎｆ２（本発明の第２の要求）を、記憶部３８５から読み出した所定の暗号鍵を用いて暗号化部３８３で暗号化した後に、受信部３８１からネットワークを介して認証装置３５１に送信する。

【０１４６】

ステップＳＴ３３：

図１５に示す認証装置３５１の制御部３９６は、認証装置３５０からの要求Ｉｎｆ２を受信部３９１が受信すると、記憶部３９５から読み出した所定の暗号鍵を用いて復号部３９４において当該要求Ｉｎｆ２を復号する。

次に、署名作成部３９７は、当該復号された要求Ｉｎｆ２に格納された受注者３３を特定する情報ｂ１に対応する受注者３３の公開鍵$K_{33,P}$を記憶部３８５から読み出し、当該公開鍵$K_{33,P}$について、記憶部３８５から読み出した自らの秘密鍵$K_{41,S}$を用いて自らの認証結果を示す署名情報Ａｕ－Ｂ（本発明の第１の署名情報）を作成する。

次に、暗号化部３９３は、受注者３３の公開鍵$K_{33,P}$および署名情報Ａｕ－Ｂを格納した応答Ｉｎｆ３を、記憶部３９５から読み出した所定の暗号鍵を用いて暗号化した後に、送信部３９２からネットワークを介して認証装置３５０に送信する。

【０１４７】

ステップＳＴ３４：

図１４に示す認証装置３５０の復号部３８４は、認証装置３５１からの応答Ｉｎｆ３を受信部３８１が受信すると、記憶部３８５から読み出した所定の暗号鍵を用いて、応答Ｉｎｆ３を復号する。

次に、署名作成部３８７は、ステップＳＴ３２で復号した要求Ｉｎｆ１から個人キー情報ｋ１を削除した情報Ｉｎｆ１’と、上記復号された応答Ｉｎｆ３に格納された署名情報Ａｕ－Ｂと、記憶部３８５から読み出した自らの公開鍵$K_{40,P}$とについて、記憶部３８５から読み出した自らの秘密鍵$K_{40,S}$を用いて署名情報Ａｕ－Ａ１を作成する。

次に、制御部３８６は、情報Ｉｎｆ１’と、署名情報Ａｕ－Ｂと、自らの公開鍵$K_{40,P}$と、上記生成した署名情報Ａｕ－Ａ１とを格納した要求Ｉｎｆ４（本発

明の第３の要求）を生成する。

次に、暗号化部３８３は、ステップＳＴ３４で認証装置３５１から受信した受注者３３の公開鍵$K_{33,P}$を用いて、上記生成した要求Ｉｎｆ４を暗号化した後に、送信部３８２から、ネットワークを介して受注者端末装置３１５に送信する。

【０１４８】

ステップＳＴ３５：

受注者端末装置３１５の復号部３７４は、認証装置３５０からの要求Ｉｎｆ４を受信部３７１が受信すると、記憶部３７５から読み出した自らの秘密鍵$K_{33,S}$を用いて、要求Ｉｎｆ４を復号する。

次に、受注者端末装置３１５の署名検証部３７７は、上記復号した要求Ｉｎｆ４に格納された署名情報Ａｕ－Ｂを、記憶部３７５から読み出した認証装置３５１の公開鍵$K_{41,P}$を用いて検証する。また、署名情報検証部は、上記復号した要求Ｉｎｆ４に格納された認証装置３５０の公開鍵$K_{40,P}$を用いて、要求Ｉｎｆ４に格納された署名情報Ａｕ－Ａ１を検証する。

【０１４９】

受注者端末装置３１５の制御部３７６は、署名検証部が上記検証の結果、署名情報Ａｕ－Ｂ，Ａｕ－Ａ１の正当性が認証されると、要求Ｉｎｆ４に格納された情報Ｉｎｆ１’と、署名情報Ａｕ－Ｂ，Ａｕ－Ａ１と、自らの個人キー情報Ｚとを格納した応答Ｉｎｆ５（本発明の所定の応答）を生成する。

次に、受注者端末装置３１５の送信部３７２は、上記生成した応答Ｉｎｆ５を、上記復号した要求Ｉｎｆ４に格納された認証装置３５０の公開鍵$K_{40,P}$を用いて復号した後に、送信部３７２から、ネットワークを介して認証装置３５０に送信する。

受注者端末装置３１５によって、署名情報Ａｕ－Ｂ，Ａｕ－Ａ１の正当性が認証されると、受注者３３は、例えば、要求Ｉｎｆ４に格納された情報Ｉｎｆ１’内の発注情報ａ１に基づいて、発注者３１が発注した商品等を発注者３１に発送したり、発注者３１が注文したサービスを発注者３１に提供する。

【０１５０】

ステップＳＴ３６：

認証装置３５０の復号部３８４は、受注者端末装置３１５からの応答Ｉｎｆ５を受信部３８１が受信すると、記憶部３８５から読み出した自らの秘密鍵$K_{40,S}$を用いて、Ｉｎｆ５を復号し、要求Ｉｎｆ１に格納された発注情報ａ１と、当該復号されたＩｎｆ５に格納された受注者３３の個人キー情報Ｚとを用いて、所定の取り引き履歴情報を作成し、これを記憶部３８５に格納する。当該履歴情報は、ネットワーク銀行３４０が、発注者３１に対して決済を行う際に用いられる。

また、認証装置３５０の署名作成部３８７は、ステップＳＴ３２で受信した要求Ｉｎｆ１と、応答Ｉｎｆ５に含まれる受注者３３の個人キー情報Ｚと、ステップＳＴ３４で作成した署名情報Ａｕ－Ａ１とについて、自らの秘密鍵$K_{40,S}$を用いて自らの認証結果を示す署名情報Ａｕ－Ａ２（本発明の第２の署名情報）を作成する。

次に、認証装置３５０の制御部３８６は、要求Ｉｎｆ１と、個人キー情報Ｚと、署名情報Ａｕ－Ａ１と、署名情報Ａｕ－Ａ２とを格納した応答Ｉｎｆ６を作成する。

【０１５１】

次に、認証装置３５０の暗号化部３８３は、上記作成した応答Ｉｎｆ６を、認証装置３５０から読み出した所定の暗号鍵を用いて暗号化した後に、送信部３８２から、ネットワークを介して発注者端末装置３１１に送信する。

発注者端末装置３１１では、受信した応答Ｉｎｆ６を、図１２に示す記憶部３６５から読み出した所定の暗号鍵を用いて復号部３６４で復号する。

次に、発注者端末装置３１１の署名検証部３６６は、当該復号した応答Ｉｎｆ６に格納された署名情報Ａｕ－Ａ１，Ａｕ－Ａ２を、記憶部３６５から読み出したネットワーク銀行３４０の公開鍵$K_{40,P}$を用いて検証することで、受注者端末装置３１５との間の当該取り引きが正当に認証されたことを確認する。

【０１５２】

以上説明したように、トランザクション認証システム３０１によれば、認証装置３５０から認証装置３５１へは、発注者３１の個人キー情報ｋ１および個人ＩＤ情報ＩＤ１を送信しないことから、発注者３１の個人情報が、発注者３１が契約していない他のネットワーク銀行３４１に漏れることを回避できる。

【０１５３】

また、トランザクション認証システム３０１によれば、認証装置３５０が、認証装置３５１から受けた受注者３３の公開鍵$K_{33,P}$および署名情報Ａｕ－Ｂを用いて、受注者３３の受注者端末装置３１５との間で直接通信を行うことで、当該取り引きの履歴を認証装置３５０に格納できる。

また、トランザクション認証システム３０１によれば、受注者３３は、自らの契約した認証装置３５０の署名情報Ａｕ－Ｂを検証することで、当該取り引きの正当性を確認できる。

また、トランザクション認証システム３０１によれば、認証装置３５０と３５１との間では、図１６に示す要求Ｉｎｆ２およびＩｎｆ３を伝送するだけで、発注者３１と受注者３３との間の取り引きを認証でき、認証装置３５０と３５１との間の通信量を小さくできる。

【０１５４】

また、トランザクション認証システム３０１によれば、図１４に示す認証装置３５０の課金処理部３８８と、図１５に示す認証装置３５１の課金処理部３９８との間で通信を行うことで、発注者３１と受注者３３との間の取り引きに関する認証に対して行う課金の割合を柔軟に決定できる。

【０１５５】

上述したように、トランザクション認証システム３０１によれば、異なる認証機関と契約をしている複数の取り引き者の間の取り引きに関する認証を、高い信頼性で、しかも効率的に行うことができる。その結果、当該認証機関と契約する契約者（取り引き者）の数を増やし、各契約者に課す会費などの費用を低額にでき、電子商取引をさらに普及させることが可能になる。

【０１５６】

本発明は上述した実施形態には限定されない。

例えば、上述した実施形態では、ネットワーク銀行３４０，３４１が、それぞれ認証装置３５０，３５１を用いて、トランザクション（取り引き）の認証業務を行う場合を例示したが、ネットワーク銀行３４０，３４１とは別の機関が、認証装置３５０，３５１を用いてトランザクションの認証業務を行うようにしても

よい。

【０１５７】

また、上述した実施形態では、発注者３１が契約したネットワーク銀行３４０の認証装置３５０と、受注者３３が契約したネットワーク銀行３４１の認証装置３５１との間で連携して認証処理を行う場合を例示したが、３人以上の取り引き者がそれぞれ異なる認証機関と契約を行っている場合に、３以上の認証装置間で連携して認証処理を行う場合にも、本発明は適用可能である。

【０１５８】

また、上述した実施形態では、図１６に示すステップＳＴ３１のように、暗号化された発注情報ａ１と、個人キー情報ｋ１および個人ＩＤ情報ＩＤ１とを含む認証要求Ｉｎｆ１を、発注者端末装置３１１から認証装置３５０に送信する場合を例示したが、発注情報ａ１および個人キー情報ｋ１を含む認証要求Ｉｎｆ１を、発注者端末装置３１１から認証装置３５０に送信してもよい。このようにすれば、課金に係わる情報である個人ＩＤ情報ＩＤ１はネットワークを介して伝送されないため、ネットワーク上で個人ＩＤ情報ＩＤ１が不正に取得され、悪用されることを回避できる。

【０１５９】

また、本発明では、例えば、認証装置３５０から受注者端末装置３１５に、署名情報Ａｕ－Ａ２（本発明の第２の署名情報）を送信するようにしてもよい。

【０１６０】

第４実施形態

図１７は、本実施形態の情報記録装置６０１の構成図である。

図１７に示すように、情報記録装置６０１は、読み出し回路６１０、暗号化回路６１１、情報分割回路６１２、書き込み回路６１３，６１４を有する。

本実施形態は、第２１、２３および２５の発明に対応した実施形態である。

情報記録装置６０１は、記録媒体６１５から読み出した個人情報Ｄ１を暗号化した後に、それぞれを単独では個人情報Ｄ１の秘匿性が保持される２つのモジュールＤ３，Ｄ４に分割し、モジュールＤ３を記録媒体６１６に書き込み、モジュールＤ４を記録媒体６１７に書き込む。

本実施形態において、記録媒体６１５，６１６，６１７は、ＨＤＤ装置や、携帯性のあるＣＤ－ＲＯＭ、フロッピーディスク、ＰＣカードなどの記録媒体である。

【０１６１】

読み出し回路６１０は、記録媒体６１５から読み出した個人情報Ｄ１を暗号化回路６１１に出力する。

個人情報Ｄ１は、図１８に示すように、情報Ｄａｔａ１～ＤａｔａＮからなる。　また、個人情報Ｄ１は、例えば、ユーザの個人ＩＤ情報や暗証番号、取り引きの履歴情報、ユーザの名前、住所、経歴および職業などの秘匿性のある情報である。

【０１６２】

暗号化回路６１１は、所定の暗号鍵を用いて、読み出し回路６１０から入力した個人情報Ｄ１を暗号化して個人情報Ｄ２を生成し、これを情報分割回路６１２に出力する。

暗号化された個人情報Ｄ２は、図１８に示すように、それぞれ情報Ｄａｔａ１～ＤａｔａＮを暗号化した情報Ｄａｔａ１’～ＤａｔａＮ’からなる。

【０１６３】

情報分割回路６１２は、暗号化回路６１１から入力した暗号化された個人情報Ｄ２を、それぞれを単独では個人情報Ｄ１の秘匿性が保持される２つのモジュールＤ３，Ｄ４に分割し、モジュールＤ３を書き込み回路６１３に出力し、モジュールＤ４を書き込み回路６１４に出力する。

図１８に示すように、情報分割回路６１２は、情報Ｄ２内の情報Ｄａｔａ１’～ＤａｔａＮ’を、それぞれ情報Ｄａｔａ１Ａ’およびＤａｔａ１Ｂ’、情報Ｄａｔａ２Ａ’およびＤａｔａ２Ｂ’、情報Ｄａｔａ３Ａ’およびＤａｔａ３Ｂ’、．．．．、情報ＤａｔａＫＡ’およびＤａｔａＫＢ’、．．．．、情報ＤａｔａＮＡ’およびＤａｔａＮＢ’に分割する。

そして、情報分割回路６１２は、情報Ｄａｔａ１Ａ’，Ｄａｔａ２Ａ’，Ｄａｔａ３Ａ’，．．．，ＤａｔａＫＡ’，．．．，ＤａｔａＮＡ’からなるモジュールＤ３を書き込み回路６１３に出力する。

また、情報分割回路６１２は、情報Ｄａｔａ１Ｂ’，Ｄａｔａ２Ｂ’，Ｄａｔａ３Ｂ’，．．．，ＤａｔａＫＢ’，．．．，ＤａｔａＮＢ’からなるモジュールＤ４を書き込み回路６１４に出力する。

【０１６４】

書き込み回路６１３は、情報分割回路６１２から入力したモジュールＤ３を記録媒体６１６に書き込む。

【０１６５】

書き込み回路６１４は、情報分割回路６１２から入力したモジュールＤ４を記録媒体６１７に書き込む。

【０１６６】

以下、情報記録装置６０１の動作を説明する。

図１９は、情報記録装置６０１の動作を説明するためのフローチャートである。

【０１６７】

ステップＳＴ８１：

読み出し回路６１０によって、記録媒体６１５から図１８に示す個人情報Ｄ１が読み出されて暗号化回路６１１に出力される。

【０１６８】

ステップＳＴ８２：

暗号化回路６１１において、所定の暗号鍵を用いて、読み出し回路６１０から入力された個人情報Ｄ１が暗号化されて図１８に示す個人情報Ｄ２が生成され、当該個人情報Ｄ２が情報分割回路６１２に出力される。

【０１６９】

ステップＳＴ８３：

情報分割回路６１２において、暗号化回路６１１から入力された個人情報Ｄ２が、それぞれを単独では個人情報Ｄ１の秘匿性が保持される図１８に示す２つのモジュールＤ３，Ｄ４に分割される。

そして、情報分割回路６１２から書き込み回路６１３にモジュールＤ３が出力され、情報分割回路６１２から書き込み回路６１４にモジュールＤ４が出力され

る。

【０１７０】

ステップＳＴ８４：

書き込み回路６１３によって、モジュールＤ３が記録媒体６１６に書き込まれる。

書き込み回路６１４によって、モジュールＤ４が記録媒体６１７に書き込まれる。

【０１７１】

以上説明したように、情報記録装置６０１によれば、図１８に示すように、個人情報Ｄ１が、暗号化された後に、それぞれを単独では個人情報Ｄ１の秘匿性が保持される２つのモジュールＤ３，Ｄ４に分割され、モジュールＤ３，Ｄ４がそれぞれ物理的に独立した記録媒体６１６，６１７にそれぞれ記録される。

そのため、記録媒体６１６，６１７を別々に保管すれば、記録媒体６１６，６１７の一方が盗難され、しかも、盗難された記録媒体に記録されているモジュールの復号が盗難者によって行われた場合でも、個人情報Ｄ１の秘匿性は保たれる。

【０１７２】

第５実施形態

図２０は、本実施形態の情報復元装置６３１の構成図である。

情報復元装置６３１は、上述した第４実施形態の情報記録装置６０１によって、記録媒体６１６と６１７とに分割して記録された個人情報から、本来の個人情報Ｄ１を復元する。

本実施形態は、第２２および２４の発明に対応した実施形態である。

図２０に示すように、情報復元装置６３１は、読み出し回路６２０，６２１、情報合成回路６２２、復号回路６２３および書き込み回路６２４を有する。

図２０において、記録媒体６１６および６１７には、前述した第４実施形態で説明した図１９に示す処理を経て、それぞれモジュールＤ３およびＤ４が記録されている。

【０１７３】

読み出し回路６２０は、記録媒体６１６から読み出したモジュールＤ３を情報合成回路６２２に出力する。

【０１７４】

読み出し回路６２１は、記録媒体６１７から読み出したモジュールＤ４を情報合成回路６２２に出力する。

【０１７５】

情報合成回路６２２は、図２１に示すように、読み出し回路６２０から入力したモジュールＤ３と、読み出し回路６２１から入力したモジュールＤ４とを合成して個人情報Ｄ２を生成し、これを復号回路６２３に出力する。

【０１７６】

復号回路６２３は、情報合成回路６２２から入力した個人情報Ｄ２を、所定の復号鍵を用いて復号して個人情報Ｄ１を生成し、これを書き込み回路６２４に出力する。

【０１７７】

書き込み回路６２４は、復号回路６２３から入力した個人情報Ｄ１を、記録媒体６１５に書き込む。

【０１７８】

以下、情報復元装置６３１の動作を説明する。

図２２は、情報復元装置６３１の動作を説明するためのフローチャートである。

【０１７９】

ステップＳＴ９１：

読み出し回路６２０によって、記録媒体６１６から図２１に示すモジュールＤ３が読み出されて情報合成回路６２２に出力される。

また、読み出し回路６２１によって、記録媒体６１７から図２１に示すモジュールＤ４が読み出されて情報合成回路６２２に出力される。

【０１８０】

ステップＳＴ９２：

情報合成回路６２２において、図２１に示すように、読み出し回路６２０から

入力したモジュールＤ３と、読み出し回路６２１から入力したモジュールＤ４とが合成されて個人情報Ｄ２が生成される。

個人情報Ｄ２は、情報合成回路６２２から復号回路６２３に出力される。

【０１８１】

ステップＳＴ９３：

復号回路６２３において、情報合成回路６２２から入力した個人情報Ｄ２が、所定の復号鍵を用いて復号して個人情報Ｄ１を生成され、これが書き込み回路６２４に出力される。

【０１８２】

ステップＳＴ９４：

書き込み回路６２４によって、復号回路６２３から入力した個人情報Ｄ１が記録媒体６１５に書き込まれる。

【０１８３】

以上説明したように、情報復元装置６３１によれば、正当な者が当該装置を用いることで、前述した第４実施形態の情報記録装置６０１によって別々の記録媒体６１６，６１７に格納されたモジュールＤ３，Ｄ４から個人情報Ｄ１を復元できる。

【０１８４】

第６実施形態

図２３は、本実施形態の情報記録装置６４１の構成図である。

図２３に示すように、情報記録装置６４１は、読み出し回路６５０、情報分割回路６５１、暗号化回路６５２，６５３および書き込み回路６５４，６５５を有する。

本実施形態は、第２１、２３および２５の発明に対応した実施形態である。

情報記録装置６４１は、記録媒体６１５から読み出した個人情報Ｄ１を、それぞれを単独では個人情報Ｄ１の秘匿性が保持される２つのモジュールＤ１２，Ｄ１３に分割した後に暗号化してモジュールＤ１４，Ｄ１５を生成し、モジュールＤ１４を記録媒体６１６に書き込み、モジュールＤ１５を記録媒体６１７に書き込む。

【０１８５】

読み出し回路６５０は、記録媒体６１５から読み出した個人情報Ｄ１を情報分割回路６５１に出力する。

個人情報Ｄ１は、図２４に示すように、情報Ｄａｔａ１～ＤａｔａＮからなる。　また、個人情報Ｄ１は、例えば、ユーザの個人ＩＤ情報や暗証番号、取り引きの履歴情報、ユーザの名前、住所、経歴および職業などの秘匿性のある情報である。

【０１８６】

情報分割回路６５１は、読み出し回路６５０から入力した個人情報Ｄ１を、それぞれを単独では個人情報Ｄ１の秘匿性が保持される２つのモジュールＤ１２，Ｄ１３に分割し、モジュールＤ１２を暗号化回路６５２に出力し、モジュールＤ１３を暗号化回路６５３に出力する。

図２４に示すように、情報分割回路６５１は、情報Ｄ１内の情報Ｄａｔａ１～ＤａｔａＮを、それぞれ情報Ｄａｔａ１ＡおよびＤａｔａ１Ｂ、情報Ｄａｔａ２ＡおよびＤａｔａ２Ｂ、情報Ｄａｔａ３ＡおよびＤａｔａ３Ｂ、．．．．、情報ＤａｔａＫＡおよびＤａｔａＫＢ、．．．．、情報ＤａｔａＮＡおよびＤａｔａＮＢに分割する。

そして、情報分割回路６５１は、情報Ｄａｔａ１Ａ，Ｄａｔａ２Ａ，Ｄａｔａ３Ａ，．．．，ＤａｔａＫＡ，．．．，ＤａｔａＮＡからなるモジュールＤ１２を暗号化回路６５２に出力する。

また、情報分割回路６５１は、情報Ｄａｔａ１Ｂ，Ｄａｔａ２Ｂ，Ｄａｔａ３Ｂ，．．．，ＤａｔａＫＢ，．．．，ＤａｔａＮＢからなるモジュールＤ１３を暗号化回路６５３に出力する。

【０１８７】

暗号化回路６５２は、所定の暗号鍵を用いて、情報分割回路６５１から入力した個人情報Ｄ１２を暗号化して個人情報Ｄ１４を生成し、これを書き込み回路６５４に出力する。

暗号化された個人情報Ｄ１４は、図２４に示すように、それぞれ情報Ｄａｔａ１Ａ～ＤａｔａＮＡを暗号化した情報Ｄａｔａ１Ａ’～ＤａｔａＮＡ’からなる

。

【０１８８】

暗号化回路６５３は、所定の暗号鍵を用いて、情報分割回路６５１から入力した個人情報Ｄ１３を暗号化して個人情報Ｄ１５を生成し、これを書き込み回路６５５に出力する。暗号化回路６５３が用いる暗号鍵は、暗号化回路６５２が用いる暗号鍵と同じものを用いてもよいし、異なるものを用いてもよい。

暗号化された個人情報Ｄ１５は、図２４に示すように、それぞれ情報ＤａｔａＩＢ～ＤａｔａＮＢを暗号化した情報ＤａｔａＩＢ’～ＤａｔａＮＢ’からなる

。

【０１８９】

書き込み回路６５４は、暗号化回路６５２から入力したモジュールＤ１４を記録媒体６１６に書き込む。

【０１９０】

書き込み回路６５５は、暗号化回路６５３から入力したモジュールＤ１５を記録媒体６１７に書き込む。

【０１９１】

以下、情報記録装置６０１の動作を説明する。

図２５は、情報記録装置６４１の動作を説明するためのフローチャートである

。

【０１９２】

ステップＳＴ１３１：

読み出し回路６５０によって、記録媒体６１５から図２４に示す個人情報Ｄ１が読み出されて情報分割回路６５１に出力される。

【０１９３】

ステップＳＴ１３２：

情報分割回路６５１において、図２４に示すように、読み出し回路６５０から入力した個人情報Ｄ１が、それぞれを単独では個人情報Ｄ１の秘匿性が保持される２つのモジュールＤ１２，Ｄ１３に分割され、モジュールＤ１２が暗号化回路６５２に出力され、モジュールＤ１３が暗号化回路６５３に出力される。

【０１９４】

ステップＳＴ１３３：

暗号化回路６５２において、図２４に示すように、所定の暗号鍵を用いて、情報分割回路６５１から入力した個人情報Ｄ１２が暗号化されて個人情報Ｄ１４が生成され、これが書き込み回路６５４に出力される。

また、暗号化回路６５３において、図２４に示すように、所定の暗号鍵を用いて、情報分割回路６５１から入力した個人情報Ｄ１３が暗号化されて個人情報Ｄ１５が生成され、これが書き込み回路６５５に出力される。

【０１９５】

ステップＳＴ１３４：

書き込み回路６５４によって、暗号化回路６５２から入力したモジュールＤ１４が記録媒体６１６に書き込まれる。

書き込み回路６５５によって、暗号化回路６５３から入力したモジュールＤ１５が記録媒体６１７に書き込まれる。

【０１９６】

以上説明したように、情報記録装置６４１によれば、図２４に示すように、個人情報Ｄ１が、それぞれを単独では個人情報Ｄ１の秘匿性が保持される２つのモジュールＤ１２，Ｄ１３に分割された後に暗号化されてモジュールＤ１４，Ｄ１５が生成され、モジュールＤ１４，Ｄ１５がそれぞれ物理的に独立した記録媒体６１６，６１７にそれぞれ記録される。

そのため、記録媒体６１６，６１７を別々に保管すれば、記録媒体６１６，６１７の一方が盗難され、しかも、盗難された記録媒体に記録されているモジュールの復号が盗難者によって行われた場合でも、個人情報Ｄ１の秘匿性は保たれる。

【０１９７】

<u>第７実施形態</u>

図２６は、本実施形態の情報復元装置６６１の構成図である。

情報復元装置６６１は、上述した第６実施形態の情報記録装置６４１によって、記録媒体６１６と６１７とに分割して記録された個人情報から、本来の個人情

報Ｄ１を復元する。

図２６に示すように、情報復元装置６６１は、読み出し回路６７０，６７１、復号回路６７２，６７３、情報合成回路６７４および書き込み回路６７５を有する。

本実施形態は、第２２および第２４の発明に対応した実施形態である。

図２６において、記録媒体６１６および６１７には、前述した第６実施形態で説明した図２５に示す処理を経て、それぞれモジュールＤ１４およびＤ１５が記録されている。

【０１９８】

読み出し回路６７０は、記録媒体６１６から読み出したモジュールＤ１４を復号回路６７２に出力する。

【０１９９】

読み出し回路６７１は、記録媒体６１７から読み出したモジュールＤ１５を復号回路６７３に出力する。

【０２００】

復号回路６７２は、読み出し回路６７０から入力したモジュールＤ１４を、所定の復号鍵を用いて復号してモジュールＤ１２を生成し、これを情報合成回路６７４に出力する。

【０２０１】

復号回路６７３は、読み出し回路６７１から入力したモジュールＤ１５を、所定の復号鍵を用いて復号してモジュールＤ１３を生成し、これを情報合成回路６７４に出力する。

【０２０２】

情報合成回路６７４は、図２７に示すように、復号回路６７２から入力したモジュールＤ１２と、復号回路６７３から入力したモジュールＤ１３とを合成して個人情報Ｄ１を生成し、これを書き込み回路６７５に出力する。

【０２０３】

書き込み回路６７５は、情報合成回路６７４から入力した個人情報Ｄ１を、記録媒体６１５に書き込む。

【０２０４】

以下、情報復元装置６６１の動作を説明する。

図２８は、情報復元装置６６１の動作を説明するためのフローチャートである。

ステップＳＴ１４１：

読み出し回路６７０によって、図２７に示すように、記録媒体６１６からモジュールＤ１４が読み出されて復号回路６７２に出力される。

また、読み出し回路６７１によって、記録媒体６１７からモジュールＤ１５が読み出されて復号回路６７３に出力される。

【０２０５】

ステップＳＴ１４２：

復号回路６７２において、読み出し回路６７０から入力したモジュールＤ１４が、所定の復号鍵を用いて復号されてモジュールＤ１２が生成され、これが情報合成回路６７４に出力される。

また、復号回路６７３において、読み出し回路６７１から入力したモジュールＤ１５が、所定の復号鍵を用いて復号されてモジュールＤ１３が生成され、これが情報合成回路６７４に出力される。

【０２０６】

ステップＳＴ１４３：

情報合成回路６７４において、図２７に示すように、復号回路６７２から入力したモジュールＤ１２と、復号回路６７３から入力したモジュールＤ１３とが合成されて個人情報Ｄ１が生成され、これが書き込み回路６７５に出力される。

【０２０７】

ステップＳＴ１４４：

書き込み回路６７５によって、情報合成回路６７４から入力された個人情報Ｄ１が、記録媒体６１５に書き込まれる。

【０２０８】

以上説明したように、情報復元装置６３１によれば、正当な者が当該装置を用いることで、前述した第６実施形態の情報記録装置６４１によって別々の記録媒体６１６，１７に格納されたモジュールＤ１４，Ｄ１５から個人情報Ｄ１を復元

できる。

【０２０９】

本発明は上述した実施形態には限定されない。

例えば、上述した実施形態では、個人情報を分割して得た複数のモジュールを異なる記録媒体に記録する場合を例示したが、当該複数のモジュールを同じ記録媒体の異なる領域に記録してもよい。この場合に、記録媒体の何れの領域に何れもモジュールを記録したかを秘密にしておけば、当該記録媒体を不正に取得した者は、記録媒体から読み出したモジュールの合成の仕方が分からず、個人情報を復元できない。

【０２１０】

また、上述した実施形態では、所定の情報を分割する前後の何れか一方で暗号化を行う場合を例示したが、所定の情報を分割する前後の何れでも暗号化を行う場合、並びに所定の情報を分割する前後の双方で暗号化を行う場合でも本発明は適用可能である。

【０２１１】

また、上述した実施形態では、本発明の所定の情報として、個人情報を例示したが、その他、映像、音声などの情報であってもよい。

【０２１２】

また、上述した実施形態では、個人情報を２分割して２つの記録媒体６１６，６１７に記録する場合を例示したが、個人情報を３分割以上して３つ以上の記録媒体に記録してもよい。

【０２１３】

第８実施形態

以下、本発明の実施形態に係わるトランザクション認証システムについて説明する。

図２９は、本実施形態のトランザクション認証システム２０１の全体構成図である。

図２９に示すように、トランザクション認証システム２０１では、例えば、発注者３１の発注者端末装置２１１と、受注者３３の受注者端末装置２１５と、ネ

ットワーク銀行２４０の認証装置２５０と、認証履歴を格納する認証履歴格納装置１４とが、インターネットなどのネットワーク（通信網）を介して接続されており、発注者３１と受注者３３との間のトランザクション（取り引き）の正当性を認証装置２５０で認証する。

なお、当該ネットワークに接続されている発注者端末装置２１１および発注者受注者端末装置２１５の数は任意である。

【０２１４】

本実施形態は、第７～第１１の発明に対応した実施形態である。

発注者端末装置２１１が第９の発明の処理装置に対応し、認証装置２５０が本発明の認証装置に対応している。

【０２１５】

本実施形態では、例えば、発注者３１および受注者３３とネットワーク銀行２４０との間で認証を行うことに関しての契約が成されている。また、発注者３１と引き落とし銀行２４２との間では、例えば、ネットワーク銀行２４０によって認証された取り引きに関しての引き落としを行う旨の契約がなされている。また、ネットワーク銀行２４０と保険会社２４３との間では、ネットワーク銀行２４０が係わった電子商取引によって生じた損害についての保険契約がなされている。

【０２１６】

以下、トランザクション認証システム２０１を構成する各装置について説明する。

〔発注者端末装置２１１〕

図３０に示すように、発注者端末装置２１１は、例えば、発注者３１の家庭などに設けられた、パーソナルコンピュータ、セット・トップ・ボックスあるいはゲーム機器などの装置であり、受信部２６１、送信部２６２、暗号化部２６３、復号部２６４、記憶部２６５、制御部２６６および署名検証部２６７を有する。

なお、発注者端末装置２１１は、例えば、発注者３１が使用する際に、発注者３１の指紋等の身体的特徴から得られる情報と、予め記憶部２６５に予め記憶してある身体的特徴を示す情報とを比較することで、発注者３１が正当な利用者で

あることを認証する生体認証部を有していてもよい。

【０２１７】

ここで、受信部２６１が第９の発明の受信手段に対応し、送信部２６２が第９の発明の送信手段に対応し、制御部２６６が第９の発明の制御手段に対応している。

【０２１８】

受信部２６１は、ネットワークを介して認証装置２５０から情報あるいは要求を受信する。

送信部２６２は、ネットワークを介して認証装置２５０に情報あるいは要求を送信する。

また、受信部２６１および送信部２６２は、受注者３３が提供する商品等の案内情報にアクセスする際に、ネットワークを介して、当該サーバ装置との間で情報あるいは要求の送受信を行う。

暗号化部２６３は、所定の暗号鍵を用いて、情報あるいは要求を暗号化する。

復号部２６４は、所定の暗号鍵を用いて、情報あるいは要求を復号する。

記憶部２６５は、製造元で受注者端末装置２１５に付された装置ＩＤ情報$ＩＤ_M$（本発明の装置識別情報）と、発注者３１が作成した秘密鍵$K_{33,S}$などを格納する。

署名検証部２６７は、例えば、認証装置２５０が作成した署名情報を、ネットワーク銀行２４０の公開鍵$K_{40,P}$を用いて検証する。

制御部２６６は、発注者端末装置２１１内の各構成要素の処理を統括的に制御する。

【０２１９】

制御部２６６は、例えば、発注者３１による操作に応じて、発注情報ａ１と、個人キー情報ｋ１（本発明の個人識別情報）と、個人ＩＤ情報ＩＤ１（本発明の個人識別情報）と、記憶部２６５から読み出した装置ＩＤ情報$ＩＤ_M$との全体に対してを暗号化を行い、もしくは個別情報毎に暗号化を行い、当該暗号化した情報を格納した認証要求Ｉｎｆ１を生成する。

また、制御部２６６は、例えば、認証要求Ｉｎｆ１を認証装置２５０に送信し

た後に、認証装置２５０から認証応答Ｉｎｆ４を受信したときに、認証応答Ｉｎｆ４に含まれる認証要求の送信元の装置を示す装置ＩＤ情報$ＩＤ_{M}$と、記憶部２６５から読み出した発注者端末装置２１１の装置ＩＤ情報$ＩＤ_{M}$とが一致するか否かを検出し、一致している場合には、正当な取り引きが行われていると判断し、不一致の場合には、不正な取り引きが行われたと判断して、その旨を受注者端末装置２１５および認証装置２５０の少なくとも一方に通知する。

【０２２０】

〔受注者端末装置２１５〕

図３１に示すように、受注者端末装置２１５は、サイバーモール(Cyber Moll)などに店舗を出している受注者３３が使用するサーバ装置であり、受信部２７１、送信部２７２、暗号化部２７３、復号部２７４、記憶部２７５、制御部２７６および署名検証部２７７を有する。

受信部２７１は、ネットワークを介して認証装置２５０から情報あるいは要求を受信する。

送信部２７２は、ネットワークを介して認証装置２５０に情報あるいは要求を送信する。

また、受信部２７１および送信部２７２は、発注者端末装置２１１からのアクセスに応じて、例えば、記憶部２７５から読み出した受注者３３が提供する商品等の案内情報を、ネットワークを介して、発注者端末装置２１１に送信する。

暗号化部２７３は、所定の暗号鍵を用いて、情報あるいは要求を暗号化する。

復号部２７４は、所定の暗号鍵を用いて、情報あるいは要求を復号する。

記憶部２７５は、受注者３３が作成した秘密鍵$K_{33,S}$などを格納する。

制御部２７６は、受注者端末装置２１５内の各構成要素の処理を統括的に制御する。

署名検証部２７７は、例えば、ネットワーク銀行２４０の公開鍵$K_{40,P}$を用いて、認証装置２５０が作成した署名情報の検証を行う。

【０２２１】

〔認証装置２５０〕

図３２に示すように、認証装置２５０は、受信部２８１、送信部２８２、暗号

化部２８３、復号部２８４、記憶部２８５、制御部２８６、署名作成部２８７および課金処理部２８８を有する。

【０２２２】

ここで、受信部２８１が第７および第８の発明の受信手段に対応し、送信部２８２が第７および第８の発明の送信手段に対応し、記憶部２８５が第７および第８の発明の記憶手段に対応し、制御部２８６が第７および第８の発明の認証処理手段に対応している。

【０２２３】

受信部２８１は、ネットワークを介して発注者端末装置２１１および受注者端末装置２１５から情報あるいは要求を受信する。

送信部２８２は、ネットワークを介して発注者端末装置２１１および受注者端末装置２１５に情報あるいは要求を送信する。

暗号化部２８３は、所定の暗号鍵を用いて、情報あるいは要求を暗号化する。

復号部２８４は、所定の暗号鍵を用いて、情報あるいは要求を復号する。

記憶部２８５は、発注者３１がネットワーク銀行２４０と契約したときに、発注者３１の個人キー情報ｋ１と、個人ＩＤ情報ＩＤ１と、発注者端末装置２１１のアドレス（または、発注者端末装置２１１が配設された家庭のセット・トップ・ボックスのアドレスあるいは電話番号等）との対応表を記憶する。また、記憶部２８５は、例えば、発注者３１および受注者３３がネットワーク銀行２４０と契約をしたときに、発注者３１が作成した秘密鍵$K_{31,S}$に対応する公開鍵$K_{31,P}$、並びに受注者３３が作成した秘密鍵$K_{33,S}$に対応する公開鍵$K_{33,P}$などを格納する。

制御部２８６は、認証装置２５０内の各構成要素の処理を統括的に制御する。

署名作成部２８７は、ネットワーク銀行２４０の秘密鍵$K_{40,S}$を用いて署名情報の作成を行う。

課金処理部２８８は、発注者３１による取り引きに関する認証に対しての課金処理を行う。

認証装置２５０の各構成要素の詳細な処理については、後述する動作例で記載する。

【０２２４】

以下、トランザクション認証システム２０１の動作例を説明する。

当該動作例を開始する前提として、発注者３１とネットワーク銀行２４０との間で所定の契約が結ばれ、ネットワーク銀行２４０は、発注者３１に対して、個人キー情報ｋ１および個人ＩＤ情報ＩＤ１を発行する。

ネットワーク銀行２４０は、個人キー情報ｋ１と、個人ＩＤ情報ＩＤ１と、発注者端末装置２１１のアドレス（または、発注者端末装置２１１が配設された家庭のセット・トップ・ボックスのアドレスあるいは電話番号等）との対応表を図３２に示す認証装置２５０の記憶部２８５に記憶する。ここで、個人キー情報ｋ１は、例えば、ネットワーク銀行２４０と契約した契約者（発注者３１）の契約番号などの個人情報を示す識別子である。また、個人ＩＤ情報ＩＤ１は、発注者３１の銀行口座番号などの課金に係わる情報を示す識別子である。

【０２２５】

また、ネットワーク銀行２４０は、自らの秘密鍵$K_{40,S}$を図３２に示す認証装置２５０の記憶部２８５に記憶すると共に、当該秘密鍵$K_{40,S}$に対応する公開鍵$K_{40,P}$を発注者端末装置２１１および受注者端末装置２１５に送信する。発注者端末装置２１１は、公開鍵$K_{40,P}$を図３０に示す記憶部２６５に記憶する。受注者端末装置２１５は、公開鍵$K_{40,P}$を図３１に示す記憶部２７５に記憶する。

【０２２６】

また、受注者３３とネットワーク銀行２４０との間で所定の契約が結ばれ、ネットワーク銀行２４０は、受注者３３に対して、個人キー情報Ｚおよび個人ＩＤ情報ＩＤ２を発行する。ネットワーク銀行２４０は、個人キー情報Ｚおよび個人ＩＤ情報ＩＤ２の対応表を図３２に示す認証装置２５０の記憶部２８５に記憶する。

【０２２７】

図３３は、トランザクション認証システム２０１の動作例を説明するための図である。

ステップＳＴ２１：

図２９に示す発注者３１は、例えばネットワーク上の商店である受注者３３に

商品を発注する場合に、発注する商品名および数量などを示す発注情報ａ１と、発注者３１の個人キー情報ｋ１と、発注者３１の個人ＩＤ情報ＩＤ１とを、図示しない操作手段を操作して発注者端末装置２１１に入力する。なお、発注情報ａ１には、受注者３３を特定する情報が含まれている。

次に、図３０に示す発注者端末装置２１１の暗号化部２６３は、記憶部２６５から読み出したネットワーク銀行２４０の公開鍵$K_{40,P}$を用いて、発注情報ａ１と、個人キー情報ｋ１と、個人ＩＤ情報ＩＤ１と、記憶部２６５から読み出した装置ＩＤ情報ID_Mとの全体に対してを暗号化を行い、当該暗号化した情報を格納した認証要求Ｉｎｆ１（本発明の第１の要求）を、送信部２６２からネットワークを介して、図２９に示すネットワーク銀行２４０の認証装置２５０に送信する。

【０２２８】

ステップＳＴ２２：

図３２に示す認証装置２５０は、発注者端末装置２１１からの認証要求Ｉｎｆ１を受信部２８１が受信すると、記憶部２８５からネットワーク銀行２４０の秘密鍵$K_{40,S}$を読み出し、復号部２８４において、当該秘密鍵$K_{40,S}$を用いて認証要求Ｉｎｆ１を復号する。

次に、認証装置２５０は、制御部２８６の制御に基づいて、上記復号した認証要求Ｉｎｆ１から個人キー情報ｋ１を削除した情報Ｉｎｆ１’について、記憶部２８５から読み出した自らの秘密鍵$K_{40,S}$を用いて署名情報Ａｕ１を作成する。

次に、認証装置２５０は、情報Ｉｎｆ１’および署名情報Ａｕ１を格納した要求Ｉｎｆ２を生成する。

次に、暗号化部２８３は、図３２に示す記憶部２８５から読み出した受注者３３の公開鍵$K_{33,P}$を用いて、上記生成した要求Ｉｎｆ２を暗号化した後に、送信部２８２から、ネットワークを介して受注者端末装置２１５に送信する。

【０２２９】

ステップＳＴ２３：

受注者端末装置２１５の復号部２７４は、認証装置２５０からの要求Ｉｎｆ２を受信部２７１が受信すると、記憶部２７５から読み出した自らの秘密鍵$K_{33,S}$

を用いて、要求Ｉｎｆ２を復号する。

次に、受注者端末装置２１５の署名検証部２７７は、上記復号した要求Ｉｎｆ２に格納された署名情報Ａｕ１を、記憶部２７５から読み出した認証装置２５０の公開鍵$K_{40,P}$を用いて検証する。

【０２３０】

受注者端末装置２１５の制御部２７６は、署名検証部が上記検証の結果、署名情報Ａｕ１の正当性が認証されると、要求Ｉｎｆ２に格納された情報Ｉｎｆ１’を図３１に示す記憶部２７５に記憶する。受注者３３は、情報Ｉｎｆ１’内の発注情報ａ１に基づいて、発注者３１への商品等の発送予定などを示す受注確認情報ｃ１を生成する。

次に、制御部２７６は、要求Ｉｎｆ２、受注確認情報ｃ１および自らの個人キー情報Ｚを格納した応答Ｉｎｆ３を生成する。

次に、受注者端末装置２１５の送信部２７２は、上記生成した応答Ｉｎｆ３を、記憶部２７５から読み出したネットワーク銀行２４０の公開鍵$K_{40,P}$を用いて暗号化部２７３で暗号化した後に、送信部２７２から、ネットワークを介して認証装置２５０に送信する。

受注者３３は、例えば、要求Ｉｎｆ２に格納された情報Ｉｎｆ１’内の発注情報ａ１に基づいて、発注者３１が発注した商品等を発注者３１に発送したり、発注者３１が注文したサービスを発注者３１に提供する。

【０２３１】

ステップＳＴ２４：

認証装置２５０の復号部２８４は、受注者端末装置２１５からの応答Ｉｎｆ３を受信部２８１が受信すると、記憶部２８５から読み出した自らの秘密鍵$K_{40,S}$を用いて、Ｉｎｆ３を復号し、要求Ｉｎｆ１に格納された発注情報ａ１と、当該復号されたＩｎｆ３に格納された受注者３３の個人キー情報Ｚとを用いて、所定の取り引き履歴情報を作成し、これを記憶部２８５に格納する。当該履歴情報は、ネットワーク銀行２４０が、発注者３１に対して決済を行う際に用いられる。

また、認証装置２５０の署名作成部２８７は、ステップＳＴ２３で受信した応答Ｉｎｆ３について、自らの秘密鍵$K_{40,S}$を用いて署名情報Ａｕ２を作成する。

次に、認証装置２５０の制御部２８６は、応答Ｉｎｆ３および署名情報Ａｕ２を格納した認証応答Ｉｎｆ４を作成する。

次に、認証装置２５０の暗号化部２８３は、上記作成し認証た応答Ｉｎｆ４を、記憶部２８５から読み出した発注者３１の公開鍵$K_{31,P}$を用いて暗号化した後に、送信部２８２から、ネットワークを介して発注者端末装置２１１に送信する。

【０２３２】

ステップＳＴ２５：

発注者端末装置２１１では、受信した認証応答Ｉｎｆ４を、図３０示す記憶部２６５から読み出した発注者３１の秘密鍵$K_{31,S}$を用いて復号部２６４で復号する。

次に、発注者端末装置２１１の署名検証部２６６は、当該復号した認証応答Ｉｎｆ４に格納された署名情報Ａｕ２を、記憶部２６５から読み出したネットワーク銀行２４０の公開鍵$K_{40,P}$を用いて検証すると共に、Ｉｎｆ４内の発注情報ａ１内に記述された装置ＩＤ情報$ＩＤ_M$が図３０に示す発注者端末装置２１１の記憶部２６５に記憶されている自らの装置ＩＤ情報$ＩＤ_M$と一致するかを判断し、一致すると判断した場合には、受注者３３との間の当該取り引きが正当に行われたことを確認する。　発注者端末装置２１１は、Ｉｎｆ４内の発注情報ａ１内に記述された装置ＩＤ情報$ＩＤ_M$が図３０に示す発注者端末装置２１１の記憶部２６５に記憶されている自らの装置ＩＤ情報$ＩＤ_M$と一致しないと判断した場合には、例えば、認証応答Ｉｎｆ４を格納した不正発注通知Ｉｎｆ５を認証装置２５０および受注者端末装置２１５の少なくとも一方に送信する。

これにより、認証装置２５０および受注者端末装置２１５は、発注者端末装置２１１が発した認証要求Ｉｎｆ１に対応した発注を取り消す。

また、発注者端末装置２１１は、不正発生通知Ｉｎｆ５を、図２９に示す引き落とし銀行２４２に送信してもよい。

【０２３３】

以上説明したように、トランザクション認証システム２０１によれば、認証要求Ｉｎｆ１内に、個人ＩＤ情報ＩＤ１の他に当該認証要求を出した装置ＩＤ情報

ID_M を自動的に挿入し、認証装置２５０において、認証要求Ｉｎｆ１に含まれる発注者３１が使用する発注者端末装置２１１のアドレスに、認証結果を含む認証応答Ｉｎｆ４を送信し、当該認証応答Ｉｎｆ４内に当該認証要求を出した装置ＩＤ情報ID_M を格納することで、発注者端末装置２１１では、認証応答Ｉｎｆ４に格納された当該認証要求を出した装置ＩＤ情報ID_M と自らの装置ＩＤ情報ID_M とが一致するか否かを判断することで、自らの個人ＩＤ情報ＩＤ１を用いた不正な認証要求（なりすまし）が発生したことを検出できる。

その結果、トランザクション認証システム２０１によれば、他人の個人ＩＤ情報を用いた不正な取り引きを効果的に抑制できる。

【０２３４】

上述したように、トランザクション認証システム１２０１によれば、電子商取引の信頼性を向上でき、当該認証機関と契約する契約者（取り引き者）の数を増やし、各契約者に課す会費などの費用を低額にでき、電子商取引をさらに普及させることが可能になる。

【０２３５】

本発明は上述した実施形態に限定されない。

例えば、上述した実施形態では、発注者端末装置２１１において、認証応答Ｉｎｆ４内の発注情報ａ１内に記述された装置ＩＤ情報ID_M が図３０に示す発注者端末装置２１１の記憶部２６５に記憶されている自らの装置ＩＤ情報ID_M と一致するかを判断し、一致しないと判断した場合には、例えば、認証応答Ｉｎｆ４を格納した不正発注通知Ｉｎｆ５を認証装置２５０および受注者端末装置２１５の少なくとも一方に送信する場合を例示したが、例えば、一致しない旨（不正な取り引きが行われた旨）を発注者端末装置２１１のディスプレイなどに表示し、発注者３１にその旨を知らせるようにしてもよい。

また、発注者端末装置２１１において、上述した装置ＩＤ情報ID_M の一致を判断するのではなく、発注者３１が判断してもよい。

また、発注者端末装置２１１が配設された家庭にホーム・ゲートウェイ(Home Gateway)が設置されている場合には、ホーム・ゲートウェイに発注者端末装置２１１の装置ＩＤ情報ID_M を登録しておき、認証装置２５０からの認証応答Ｉｎ

ｆ４をホーム・ゲートウェイが受信したときに、ホーム・ゲート・ウェイにおいて、上記装置ＩＤ情報$ＩＤ_{M}$の一致の判断を行ってもよい。

【０２３６】

また、上述した実施形態では、ネットワーク銀行２４０が、認証装置２５０を用いて、トランザクション（取り引き）の認証業務を行う場合を例示したが、ネットワーク銀行２４０とは別の機関が、認証装置２５０を用いてトランザクションの認証業務を行うようにしてもよい。

【０２３７】

また、上述した実施形態では、図３３に示すステップＳＴ２１のように、暗号化された発注情報ａ１と、個人キー情報ｋ１と、個人ＩＤ情報ＩＤ１と、装置ＩＤ情報$ＩＤ_{M}$とを含む認証要求Ｉｎｆ１を、発注者端末装置２１１から認証装置２５０に送信する場合を例示したが、発注情報ａ１と、個人キー情報ｋ１と、装置ＩＤ情報$ＩＤ_{M}$とを含む認証要求Ｉｎｆ１を、発注者端末装置２１１から認証装置２５０に送信してもよい。このようにすれば、課金に係わる情報である個人ＩＤ情報ＩＤ１はネットワークを介して伝送されないため、ネットワーク上で個人ＩＤ情報ＩＤ１が不正に取得され、悪用されることを回避できる。

【０２３８】

また、上述した実施形態では、図３０に示す発注者端末装置２１１の暗号化部２６３において、記憶部２６５から読み出した所定の暗号鍵を用いて、発注情報ａ１と、個人キー情報ｋ１と、個人ＩＤ情報ＩＤ１と、記憶部２６５から読み出した装置ＩＤ情報$ＩＤ_{M}$との全体に対してを暗号化を行う場合を例示したが、発注情報ａ１と、個人キー情報ｋ１と、個人ＩＤ情報ＩＤ１と、記憶部２６５から読み出した装置ＩＤ情報$ＩＤ_{M}$とのそれぞれについて個別に暗号化を行ってもよい。

【０２３９】

第９実施形態

図３４は、本実施形態のトランザクション認証システム４０１の全体構成図である。

図３４に示すように、トランザクション認証システム４０１では、例えば、発

注者３１の発注者端末装置４１１と、受注者３３の受注者端末装置４１５と、ネットワーク銀行４４０の認証装置４５０と、認証履歴を格納する認証履歴格納装置１４とが、インターネットなどのネットワーク（通信網）を介して接続されており、発注者３１と受注者３３との間のトランザクション（取り引き）の正当性を認証装置４５０で認証する。

なお、当該ネットワークに接続されている発注者端末装置４１１および受注者端末装置４１５の数は任意である。

【０２４０】

本実施形態では、認証装置４５０が第１５の発明の通信装置、並びに第１６および第１７の発明の第１の通信装置に対応し、受注者端末装置４１５あるいは不正者端末装置４５６が第１６および第１７の発明の第２の通信装置に対応している。

【０２４１】

本実施形態では、例えば、発注者３１および受注者３３とネットワーク銀行４４０との間で認証を行うことに関しての契約が成されている。また、発注者３１と引き落とし銀行４４２との間では、例えば、ネットワーク銀行４４０によって認証された取り引きに関しての引き落としを行う旨の契約がなされている。また、ネットワーク銀行４４０と保険会社４４３との間では、ネットワーク銀行４４０が係わった電子商取引によって生じた損害についての保険契約がなされている。

【０２４２】

以下、トランザクション認証システム４０１を構成する各装置について説明する。

〔発注者端末装置４１１〕

図３５に示すように、発注者端末装置４１１は、例えば、発注者３１の家庭などに設けられた、パーソナルコンピュータ、セット・トップ・ボックスあるいはゲーム機器などの装置であり、受信部４６１、送信部４６２、暗号化部４６３、復号部４６４、記憶部４６５、制御部４６６および署名検証部４６７を有する。

なお、発注者端末装置４１１は、例えば、発注者３１が使用する際に、発注者

３１の指紋等の身体的特徴から得られる情報と、予め記憶部４６５に予め記憶してある身体的特徴を示す情報とを比較することで、発注者３１が正当な利用者であることを認証する生体認証部を有していてもよい。

【０２４３】

ここで、受信部４６１が第１６の発明の第２の受信手段に対応し、送信部４６２が第１６の発明の第２の送信手段に対応している。

【０２４４】

受信部４６１は、ネットワークを介して認証装置４５０から情報あるいは要求を受信する。

送信部４６２は、ネットワークを介して認証装置４５０に情報あるいは要求を送信する。

また、受信部４６１および送信部４６２は、受注者３３が提供する商品等の案内情報にアクセスする際に、ネットワークを介して、当該サーバ装置との間で情報あるいは要求の送受信を行う。

暗号化部４６３は、所定の暗号鍵を用いて、情報あるいは要求を暗号化する。

復号部４６４は、所定の暗号鍵を用いて、情報あるいは要求を復号する。

記憶部４６５は、発注者３１が作成した秘密鍵$K_{31,S}$などを格納する。

署名検証部４６７は、例えば、認証装置４５０が作成した署名情報を、ネットワーク銀行４４０の公開鍵$K_{40,P}$を用いて検証する。

制御部４６６は、発注者端末装置４１１内の各構成要素の処理を統括的に制御する。

【０２４５】

制御部４６６は、例えば、発注者３１による操作に応じて、発注情報ａ１と、個人キー情報ｋ１（本発明の利用者を識別するための個人識別情報）と、個人ＩＤ情報ＩＤ１（本発明の個人識別情報）との全体に対してを暗号化を行い、もしくは個別情報毎に暗号化を行い、当該暗号化した情報を格納した認証要求Ｉｎｆ１を生成する。

ここで、個人キー情報ｋ１および個人ＩＤ情報ＩＤ１は、発注者３１がネットワーク銀行４４０に自らを登録したときに、当該発注者３１に割り当てられた固

有の識別子である。例えば、個人キー情報ｋ１は、ネットワーク銀行４４０と契約した契約者（発注者３１）の契約番号などの個人情報を示す識別子である。また、個人ＩＤ情報ＩＤ１は、発注者３１の銀行口座番号などの課金に係わる情報を示す識別子である。

また、制御部４６６は、例えば、認証要求Ｉｎｆ１を認証装置４５０に送信した後に、認証装置４５０から認証応答Ｉｎｆ４を受信したときに、認証応答Ｉｎｆ４に含まれる認証結果を所定の表示装置や音声出力装置を介して出力する制御を行なう。

【０２４６】

〔受注者端末装置４１５〕

図３６に示すように、受注者端末装置４１５は、サイバーモール(Cyber Mall)などに店舗を出している受注者３３が使用するサーバ装置であり、受信部４７１、送信部４７２、暗号化部４７３、復号部４７４、記憶部４７５、制御部４７６および署名検証部４７７を有する。

受信部４７１は、ネットワークを介して認証装置４５０から情報あるいは要求を受信する。

送信部４７２は、ネットワークを介して認証装置４５０に情報あるいは要求を送信する。

また、受信部４７１および送信部４７２は、発注者端末装置４１１からのアクセスに応じて、例えば、記憶部４７５から読み出した受注者３３が提供する商品等の案内情報を、ネットワークを介して、発注者端末装置４１１に送信する。

暗号化部４７３は、所定の暗号鍵を用いて、情報あるいは要求を暗号化する。

復号部４７４は、所定の暗号鍵を用いて、情報あるいは要求を復号する。

記憶部４７５は、受注者３３が作成した秘密鍵$K_{33,S}$などを格納する。

制御部４７６は、受注者端末装置４１５内の各構成要素の処理を統括的に制御する。

署名検証部４７７は、例えば、ネットワーク銀行４４０の公開鍵$K_{40,P}$を用いて、認証装置４５０が作成した署名情報の検証を行う。

【０２４７】

〔認証装置４５０〕

図３７に示すように、認証装置４５０は、受信部４８１、送信部４８２、暗号化部４８３、復号部４８４、記憶部４８５、制御部４８６、署名作成部４８７および課金処理部４８８を有する。

【０２４８】

ここで、受信部４８１が、第１５の発明の受信手段、並びに第１６の発明の第１の受信手段に対応している。送信部４８２が、第１５の発明の送信手段、並びに第１６の発明の第１の送信手段に対応している。記憶部４８５が、第１５の発明および第１６の発明の記憶手段に対応している。制御部４８６が、第１５の発明および第１６の発明の処理手段に対応している。

【０２４９】

受信部４８１は、ネットワークを介して発注者端末装置４１１および受注者端末装置４１５から情報あるいは要求を受信する。

送信部４８２は、ネットワークを介して発注者端末装置４１１および受注者端末装置４１５に情報あるいは要求を送信する。

暗号化部４８３は、所定の暗号鍵を用いて、情報あるいは要求を暗号化する。

復号部４８４は、所定の暗号鍵を用いて、情報あるいは要求を復号する。

記憶部４８５は、発注者３１がネットワーク銀行４４０と契約したときに、発注者３１の個人キー情報ｋ１と、個人ＩＤ情報ＩＤ１と、発注者３１のネットワークＩＤ＿Ｎ（本発明の送信先の情報）との対応表を図３７に示す認証装置４５０の記憶部４８５に記憶する。

ここで、ネットワークＩＤ＿Ｎは、発注者３１がネットワーク銀行４４０にオフラインで登録した、当該ネットワークのユーザである発注者３１をネットワーク内で一意に識別するための識別子である。

また、記憶部４８５は、例えば、発注者３１および受注者３３がネットワーク銀行４４０と契約をしたときに、発注者３１が作成した秘密鍵$K_{31,S}$に対応する公開鍵$K_{31,P}$、並びに受注者３３が作成した秘密鍵$K_{33,S}$に対応する公開鍵$K_{33,P}$などを格納する。

制御部４８６は、認証装置４５０内の各構成要素の処理を統括的に制御する。

署名作成部４８７は、ネットワーク銀行４４０の秘密鍵$K_{40,S}$を用いて署名情報の作成を行う。

課金処理部４８８は、発注者３１による取り引きに関する認証に対しての課金処理を行う。

認証装置４５０の各構成要素の詳細な処理については、後述する動作例で記載する。

【０２５０】

以下、トランザクション認証システム４０１の動作例を説明する。

当該動作例を開始する前提として、発注者３１とネットワーク銀行４４０との間で所定の契約が結ばれ、ネットワーク銀行４４０は、発注者３１に対して、個人キー情報ｋ１および個人ＩＤ情報ＩＤ１を発行している。

また、発注者３１は、ネットワーク内で当該発注者３１を識別するネットワークＩＤ＿Ｎを、秘密が保持される環境、例えばオフラインでネットワーク銀行４４０に登録している。

ネットワーク銀行４４０は、個人キー情報ｋ１と、個人ＩＤ情報ＩＤ１と、発注者３１のネットワークＩＤ＿Ｎとの対応表を図３７に示す認証装置４５０の記憶部４８５に記憶している。

【０２５１】

また、ネットワーク銀行４４０は、自らの秘密鍵$K_{40,S}$を図３７に示す認証装置４５０の記憶部４８５に記憶すると共に、当該秘密鍵$K_{40,S}$に対応する公開鍵$K_{40,P}$を発注者端末装置４１１および受注者端末装置４１５に送信する。発注者端末装置４１１は、公開鍵$K_{40,P}$を図３５に示す記憶部４６５に記憶する。受注者端末装置４１５は、公開鍵$K_{40,P}$を図３６に示す記憶部４７５に記憶する。

【０２５２】

また、受注者３３とネットワーク銀行４４０との間で所定の契約が結ばれ、ネットワーク銀行４４０は、受注者３３に対して、個人キー情報Ｚおよび個人ＩＤ情報ＩＤ２を発行する。ネットワーク銀行４４０は、個人キー情報Ｚおよび個人ＩＤ情報ＩＤ２の対応表を図３７に示す認証装置４５０の記憶部４８５に記憶する。

【０２５３】

以下、発注者３１が、認証装置４５０に認証要求を行なった場合のトランザクション認証システム４０１の動作を説明する。

図３８は、トランザクション認証システム４０１の当該動作を説明するための図である。

ステップＳＴ４１：

図３４に示す発注者３１は、例えばネットワーク上の商店である受注者３３に商品を発注する場合に、発注する商品名および数量などを示す発注情報ａ１と、発注者３１の個人キー情報ｋ１と、発注者３１の個人ＩＤ情報ＩＤ１とを、図示しない操作手段を操作して発注者端末装置４１１に入力する。なお、発注情報ａ１には、受注者３３を特定する情報が含まれている。

次に、図３５に示す発注者端末装置４１１の暗号化部４６３は、記憶部４６５から読み出したネットワーク銀行４４０の公開鍵$K_{40,P}$を用いて、発注情報ａ１と、個人キー情報ｋ１と、個人ＩＤ情報ＩＤ１との全体に対してを暗号化を行い、当該暗号化した情報を格納した認証要求Ｉｎｆ１（本発明の要求）を、送信部４６２からネットワークを介して、図３４に示すネットワーク銀行４４０の認証装置４５０に送信する。

【０２５４】

ステップＳＴ４２：

図３７に示す認証装置４５０は、発注者端末装置４１１からの認証要求Ｉｎｆ１を受信部４８１が受信すると、記憶部４８５からネットワーク銀行４４０の秘密鍵$K_{40,S}$を読み出し、復号部４８４において、当該秘密鍵$K_{40,S}$を用いて認証要求Ｉｎｆ１を復号する。

次に、認証装置４５０は、制御部４８６の制御に基づいて、上記復号した認証要求Ｉｎｆ１から個人キー情報ｋ１を削除した情報Ｉｎｆ１’とについて、記憶部４８５から読み出した自らの秘密鍵$K_{40,S}$を用いて署名情報Ａｕ１を作成する。

次に、認証装置４５０は、情報Ｉｎｆ１’および署名情報Ａｕ１を格納した要求Ｉｎｆ２を生成する。

次に、暗号化部４８３は、図３７に示す記憶部４８５から読み出した受注者３３の公開鍵$K_{33,P}$を用いて、上記生成した要求Ｉｎｆ２を暗号化した後に、送信部４８２から、ネットワークを介して受注者端末装置４１５に送信する。

【０２５５】

ステップＳＴ４３：

受注者端末装置４１５の復号部４７４は、認証装置４５０からの要求Ｉｎｆ２を受信部４７１が受信すると、記憶部４７５から読み出した自らの秘密鍵$K_{33,S}$を用いて、要求Ｉｎｆ２を復号する。

次に、受注者端末装置４１５の署名検証部４７７は、上記復号した要求Ｉｎｆ２に格納された署名情報Ａｕ１を、記憶部４７５から読み出した認証装置４５０の公開鍵$K_{40,P}$を用いて検証する。

【０２５６】

受注者端末装置４１５の制御部４７６は、署名検証部が上記検証の結果、署名情報Ａｕ１の正当性が認証されると、要求Ｉｎｆ２に格納された情報Ｉｎｆ１’を図３６に示す記憶部４７５に記憶する。受注者３３は、情報Ｉｎｆ１’内の発注情報ａ１に基づいて、発注者３１への商品等の発送予定などを示す受注確認情報ｃ１を生成する。

次に、制御部４７６は、要求Ｉｎｆ２、受注確認情報ｃ１および自らの個人キー情報Ｚを格納した応答Ｉｎｆ３を生成する。

次に、受注者端末装置４１５の送信部４７２は、上記生成した応答Ｉｎｆ３を、記憶部４７５から読み出したネットワーク銀行４４０の公開鍵$K_{40,P}$を用いて暗号化部４７３で暗号化した後に、送信部４７２から、ネットワークを介して認証装置４５０に送信する。

受注者３３は、例えば、要求Ｉｎｆ２に格納された情報Ｉｎｆ１’内の発注情報ａ１に基づいて、発注者３１が発注した商品等を発注者３１に発送したり、発注者３１が注文したサービスを発注者３１に提供する。

【０２５７】

ステップＳＴ４４：

認証装置４５０の復号部４８４は、受注者端末装置４１５からの応答Ｉｎｆ３

を受信部４８１が受信すると、記憶部４８５から読み出した自らの秘密鍵$K_{40,S}$を用いて、Ｉｎｆ３を復号し、要求Ｉｎｆ１に格納された発注情報ａ１と、当該復号されたＩｎｆ３に格納された受注者３３の個人キー情報Ｚとを用いて、所定の取り引き履歴情報を作成し、これを記憶部４８５に格納する。当該履歴情報は、ネットワーク銀行４４０が、発注者３１に対して決済を行う際に用いられる。

また、認証装置４５０の署名作成部４８７は、ステップＳＴ４３で受信した応答Ｉｎｆ３について、自らの秘密鍵$K_{40,S}$を用いて署名情報Ａｕ２を作成する。

次に、認証装置４５０の制御部４８６は、応答Ｉｎｆ３および署名情報Ａｕ２を格納した認証応答Ｉｎｆ４を作成する。

次に、認証装置４５０の暗号化部４８３は、上記作成し認証た応答Ｉｎｆ４を、公開鍵$K_{31,P}$を用いて暗号化した後に、個人ＩＤ情報ＩＤ１に対応する記憶部４８５から読み出した発注者３１のネットワークＩＤ＿Ｎに基づいて送信先を特定して、送信部４８２からネットワークを介して発注者端末装置４１１に送信する。

【０２５８】

発注者端末装置４１１では、受信した認証応答Ｉｎｆ４を、図３５に示す記憶部４６５から読み出した発注者３１の秘密鍵$K_{31,S}$を用いて復号部４６４で復号する。

次に、発注者端末装置４１１の署名検証部４６６は、当該復号した認証応答Ｉｎｆ４に格納された署名情報Ａｕ２を、記憶部４６５から読み出したネットワーク銀行４４０の公開鍵$K_{40,P}$を用いて検証する。

当該検証によってその正当性が確認されると、制御部４６６は、認証応答Ｉｎｆ４に格納されている発注情報ａ１や取り引きの内容を示す情報に応じた出力を、発注者端末装置４１１の図示しないディスプレイやスピーカから出力する。

【０２５９】

以下、発注者３１の個人ＩＤ１および個人キーｋ１を不正に取得した図３４に示す不正者５５が自らの端末装置である不正者端末装置４５６を用いて、認証装置４５０に認証要求を送信した場合のトランザクション認証システム４０１の動作を説明する。

ここで、不正者端末装置４５６の構成は、例えば、図３５に示す発注者端末装置４１１と同じである。

図３９は、トランザクション認証システム４０１の当該動作を説明するための図である。

ステップＳＴ５１：

図３４に示す不正者５５は、受注者３３に商品を発注する場合に、発注する商品名および数量などを示す発注情報ａ１と、不正に取得した発注者３１の個人キー情報ｋ１と、不正に取得した発注者３１の個人ＩＤ情報ＩＤ１とを、図示しない操作手段を操作して不正者端末装置４５６に入力する。

次に、不正者端末装置４５６の図３５に示す暗号化部４６３は、記憶部４６５から読み出したネットワーク銀行４４０の公開鍵$K_{40,P}$を用いて、発注情報ａ１と、個人キー情報ｋ１と、個人ＩＤ情報ＩＤ１との全体に対してを暗号化を行い、当該暗号化した情報を格納した認証要求Ｉｎｆ１を、送信部４６２からネットワークを介して、図３４に示すネットワーク銀行４４０の認証装置４５０に送信する。

【０２６０】

ステップＳＴ５２：

図３７に示す認証装置４５０は、不正者端末装置４５６からの認証要求Ｉｎｆ１を受信部４８１が受信すると、当該認証要求Ｉｎｆ１について、前述したステップＳＴ４２と同様の処理を行なう。

【０２６１】

ステップＳＴ５３：

ステップＳＴ５３の処理は、前述したステップＳＴ４３の処理と同じである。

【０２６２】

ステップＳＴ５４：

ステップＳＴ５４の処理は、前述したステップＳＴ４４の処理と同じである。

すなわち、不正者５５が不正者端末装置４５６を用いて、認証要求Ｉｎｆ１を認証装置４５０に送信した場合でも、その応答である認証応答Ｉｎｆ４は、認証装置４５０の記憶部４８５に記憶されている発注者３１のネットワークＩＤ＿Ｎ

に基づいて、発注者端末装置４１１に送信される。

これにより、発注者３１は、受信した認証応答Ｉｎｆ４に基づいて、自らが個人ＩＤ情報ＩＤ１を用いた不正な認証要求が行なわれたことを知ることができ、その旨をネットワーク銀行４４０などに通知する。

【０２６３】

以上説明したように、トランザクション認証システム４０１によれば、認証装置４５０は、発注者３１がネットワーク銀行４４０にオフラインで登録したネットワークＩＤ＿Ｎによって指定された送信先に、認証応答Ｉｎｆ４を送信するため、例えば、発注者３１の個人情報ＩＤ１を不正に取得した者が当該個人情報ＩＤ１を用いて認証装置４５０に認証要求を行なった場合に、認証装置４５０に登録されたネットワークＩＤ＿Ｎに基づいて認証装置４５０から発注者端末装置４１１に送信された認証応答Ｉｎｆ４によって、発注者３１は自らの個人情報ＩＤ１を用いた不正な取り引きが行なわれることを知ることができる。

そのため、トランザクション認証システム４０１によれば、他人の個人ＩＤ情報を用いた不正な取り引きを効果的に抑制できる。

【０２６４】

上述したように、トランザクション認証システム４０１によれば、電子商取引の信頼性を向上でき、当該認証機関と契約する契約者（取り引き者）の数を増やし、各契約者に課す会費などの費用を低額にでき、電子商取引をさらに普及させることが可能になる。

【０２６５】

本発明は上述した実施形態に限定されない。

例えば、上述した実施形態では、本発明の処理手段が行う処理として認証処理を例示したが、その他、課金処理などの処理を行う場合にも本発明は適用可能である。

【０２６６】

また、上述した実施形態では、ネットワーク銀行４４０が、認証装置４５０を用いて、トランザクション（取り引き）の認証業務を行う場合を例示したが、ネットワーク銀行４４０とは別の機関が、認証装置４５０を用いてトランザクショ

ンの認証業務を行うようにしてもよい。

【０２６７】

第１０実施形態

図４０は、本実施形態のトランザクション認証システム５０１の全体構成図である。

図４０に示すように、トランザクション認証システム５０１では、例えば、発注者３１の発注者端末装置５１１と、受注者３３の受注者端末装置５１５と、ネットワーク銀行５４０の認証装置５５０と、認証履歴を格納する認証履歴格納装置１４とが、インターネットなどの外部ネットワーク（通信網）５０９を介して接続されており、発注者３１と受注者３３との間のトランザクション（取り引き）の正当性を認証装置５５０で認証する。

なお、当該外部ネットワーク５０９に接続されているホームネットワークシステム（発注者端末システム）１０および受注者端末装置５１５の数は任意である。

【０２６８】

本実施形態は、第１８～２０の発明に対応した実施形態である。

本実施形態では、ホームネットワークシステム５１０が本発明の通信制御装置に対応し、端末装置５１１_1～５１１_4が本発明の第１の通信装置に対応し、認証装置５５０が本発明の第２の通信装置に対応している。

【０２６９】

本実施形態では、例えば、発注者３１および受注者３３とネットワーク銀行５４０との間で認証を行うことに関しての契約が成されている。また、発注者３１と引き落とし銀行５４２との間では、例えば、ネットワーク銀行５４０によって認証された取り引きに関しての引き落としを行う旨の契約がなされている。また、ネットワーク銀行５４０と保険会社５４３との間では、ネットワーク銀行５４０が係わった電子商取引によって生じた損害についての保険契約がなされている。

【０２７０】

以下、トランザクション認証システム５０１を構成する各装置について説明す

る。

〔ホームネットワークシステム５１０〕

図４０および図４１に示すように、ホームネットワークシステム５１０は、発注者３１の各家庭などに構築されており、ホームネットワークシステム５１０のホームゲートウェイ５１２が、図４０に示す受注者端末装置５１５および認証装置５５０が接続される外部ネットワーク５０９に有線あるいは無線で接続されている。

また、ホームゲートウェイ５１２には、例えば、家庭内の内部ネットワーク１３を介して、端末装置511_1，511_2，511_3，511_4が有線あるいは無線で接続される。

端末装置511_1～511_4は、例えば、デジタルテレビ受信装置、パーソナルコンピュータ、電話機およびゲーム機などである。

端末装置511_1～511_4の各々には、例えば製造元で当該端末装置を識別するための装置ＩＤ情報が割り当てられており、当該装置ＩＤ情報が各端末装置の内部メモリに記憶されている。例えば、端末装置511_1には装置ＩＤ情報ID_{M1}が割り当てられ、端末装置511_2には装置ＩＤ情報ID_{M2}が割り当てられ、端末装置511_3には装置ＩＤ情報ID_{M3}が割り当てられ、端末装置511_4には装置ＩＤ情報ID_{M4}が割り当てられている。

【０２７１】

図４２は、ホームゲートウェイ５１２の構成図である。

ホームゲートウェイ５１２は、例えば、外部ネットワークＩ／Ｆ５６１、内部ネットワークＩ／Ｆ５６２、暗号化部５６３、復号部５６４、記憶部５６５、制御部５６６および署名検証部５６７を有する。

ここで、外部ネットワークＩ／Ｆ５６１および内部ネットワークＩ／Ｆ５６２が、第１８の発明の送信手段および受信手段、並びに第１９の発明の第１の送信手段および第２の受信手段に対応している。また、記憶部５６５が、第１８の発明の記憶手段および第１９の発明の第１の記憶手段に対応している。また、制御部５６６が第１８の発明および第１９の発明の制御手段に対応している。

【０２７２】

外部ネットワークＩ／Ｆ５６１は、外部ネットワーク５０９を介して認証装置５５０との間で、情報あるいは要求の送受信を行なう。

内部ネットワークＩ／Ｆ５６２は、内部ネットワーク１３を介して端末装置５１１$_1$～５１１$_4$との間で、情報あるいは要求の送受信を行なう。

暗号化部５６３は、所定の暗号鍵を用いて、情報あるいは要求を暗号化する。

復号部５６４は、所定の暗号鍵を用いて、情報あるいは要求を復号する。

記憶部５６５は、例えば、ホームゲートウェイ５１２の電源が投入されたときに電源がオンになっている端末装置５１１$_1$～５１１$_4$から内部ネットワーク１３を介して受信した装置ＩＤ情報ID_{M1}～ID_{M4}を記憶している。

また、記憶部５６５は、発注者３１が作成した秘密鍵$K_{31,S}$などを格納する。

署名検証部５６７は、例えば、認証装置５５０が作成した署名情報を、ネットワーク銀行５４０の公開鍵$K_{40,P}$を用いて検証する。

制御部５６６は、発注者端末装置５１１内の各構成要素の処理を統括的に制御する。

制御部５６６は、ホームゲートウェイ５１２を介した端末装置５１１$_1$～５１１$_4$と認証装置５５０との間の通信の履歴を示す履歴情報を生成し、これを記憶部５６５に記憶する。

そのため、記憶部５６５に記憶された履歴情報にアクセスを行うだけで、家庭内に設けられた端末装置５１１$_1$～５１１$_4$を用いた通信の履歴を簡単に知ることができ、管理が容易になる。

【０２７３】

また、制御部５６６は、例えば、待機状態（スタンバイ状態）になっている端末装置５１１$_1$～５１１$_4$に対してのアクセスを、外部ネットワーク５０９を介して受けた場合に、対応する端末装置５１１$_1$～５１１$_4$が動作状態になるように制御する。

【０２７４】

制御部５６６は、例えば、発注者３１による操作に応じて端末装置５１１$_1$～５１１$_4$から内部ネットワークＩ／Ｆ５６２が受信した、発注情報ａ１と、個人キー情報ｋ１と（本発明の個人識別情報）、個人ＩＤ情報ＩＤ１（本発明の個人

識別情報）と、装置ＩＤ情報$ＩＤ_{M1}$～$ＩＤ_{M4}$（本発明の装置識別情報）との全体に対してを暗号化を行い、もしくは個別情報毎に暗号化を行い、当該暗号化した情報を格納した認証要求Ｉｎｆ１を生成する。

また、制御部５６６は、例えば、認証要求Ｉｎｆ１を認証装置５５０に送信した後に、認証装置５５０から認証応答Ｉｎｆ４を受信したときに、認証応答Ｉｎｆ４に含まれる認証要求の送信元の装置を示す装置ＩＤ情報と、記憶部５６５から読み出した装置ＩＤ情報$ＩＤ_{M1}$～$ＩＤ_{M4}$の何れかとが一致するか否かを検出し、一致している場合には、正当な取り引きが行われていると判断し、不一致の場合には、不正な取り引きが行われたと判断して、その旨を受注者端末装置５１５および認証装置５５０の少なくとも一方に通知する。

【０２７５】

〔受注者端末装置５１５〕

図４３に示すように、受注者端末装置５１５は、サイバーモール(Cyber Moll)などに店舗を出している受注者３３が使用するサーバ装置であり、受信部５７１、送信部５７２、暗号化部５７３、復号部５７４、記憶部５７５、制御部５７６および署名検証部５７７を有する。

受信部５７１は、外部ネットワーク５０９を介して認証装置５５０から情報あるいは要求を受信する。

送信部５７２は、外部ネットワーク５０９を介して認証装置５５０に情報あるいは要求を送信する。

また、受信部５７１および送信部５７２は、発注者端末装置５１１からのアクセスに応じて、例えば、記憶部５７５から読み出した受注者３３が提供する商品等の案内情報を、ネットワークを介して、発注者端末装置５１１に送信する。

暗号化部５７３は、所定の暗号鍵を用いて、情報あるいは要求を暗号化する。

復号部５７４は、所定の暗号鍵を用いて、情報あるいは要求を復号する。

記憶部５７５は、受注者３３が作成した秘密鍵$K_{33,S}$などを格納する。

制御部５７６は、受注者端末装置５１５内の各構成要素の処理を統括的に制御する。

署名検証部５７７は、例えば、ネットワーク銀行５４０の公開鍵$K_{40,P}$を用い

て、認証装置５５０が作成した署名情報の検証を行う。

【０２７６】

〔認証装置５５０〕

図４４に示すように、認証装置５５０は、受信部５８１、送信部５８２、暗号化部５８３、復号部５８４、記憶部５８５、制御部５８６、署名作成部５８７および課金処理部５８８を有する。

【０２７７】

ここで、受信部５８１が第１９の発明の第２の受信手段に対応し、送信部５８２が第１９の発明の第２の送信手段に対応し、記憶部５８５が第１９の発明の第２の記憶手段に対応し、制御部５８６が第１９の発明の処理手段に対応している。

【０２７８】

受信部５８１は、外部ネットワーク５０９を介してホームゲートウェイ５１２および受注者端末装置５１５から情報あるいは要求を受信する。

送信部５８２は、外部ネットワーク５０９を介してホームゲートウェイ５１２および受注者端末装置５１５に情報あるいは要求を送信する。

暗号化部５８３は、所定の暗号鍵を用いて、情報あるいは要求を暗号化する。

復号部５８４は、所定の暗号鍵を用いて、情報あるいは要求を復号する。

記憶部５８５は、発注者３１がネットワーク銀行５４０と契約したときに、発注者３１の個人キー情報ｋ１と、個人ＩＤ情報ＩＤ１と、ホームゲートウェイ５１２のアドレスとの対応表を記憶する。また、記憶部５８５は、例えば、発注者３１および受注者３３がネットワーク銀行５４０と契約をしたときに、発注者３１が作成した秘密鍵$K_{31,S}$に対応する公開鍵$K_{31,P}$、並びに受注者３３が作成した秘密鍵$K_{33,S}$に対応する公開鍵$K_{33,P}$などを格納する。

制御部５８６は、認証装置５５０内の各構成要素の処理を統括的に制御する。

署名作成部５８７は、ネットワーク銀行５４０の秘密鍵$K_{40,S}$を用いて署名情報の作成を行う。

課金処理部５８８は、発注者３１による取り引きに関する認証に対しての課金処理を行う。

認証装置５５０の各構成要素の詳細な処理については、後述する動作例で記載する。

【０２７９】

以下、トランザクション認証システム５０１の動作例を説明する。

当該動作例では、図４０に示す発注者３１が図４１に示す端末装置511_1を操作して、受注者３３が提供する商品またはサービスの発注を行なう場合を説明する。

なお、当該動作例を開始する前提として、以下の手続および処理が行なわれている。

すなわち、発注者３１とネットワーク銀行５４０との間で所定の契約が結ばれ、ネットワーク銀行５４０は、発注者３１に対して、個人キー情報ｋ１および個人ＩＤ情報ＩＤ１を発行する。

ネットワーク銀行５４０は、個人キー情報ｋ１と、個人ＩＤ情報ＩＤ１と、ホームゲートウェイ５１２のアドレスとの対応表を図４４に示す認証装置５５０の記憶部５８５に記憶する。ここで、個人キー情報ｋ１は、例えば、ネットワーク銀行５４０と契約した契約者（発注者３１）の契約番号などの個人情報を示す識別子である。また、個人ＩＤ情報ＩＤ１は、発注者３１の銀行口座番号などの課金に係わる情報を示す識別子である。

【０２８０】

また、ネットワーク銀行５４０は、自らの秘密鍵$K_{40,S}$を図４４に示す認証装置５５０の記憶部５８５に記憶すると共に、当該秘密鍵$K_{40,S}$に対応する公開鍵$K_{40,P}$をホームゲートウェイ５１２および受注者端末装置５１５に送信する。ホームゲートウェイ５１２は、公開鍵$K_{40,P}$を図４２に示す記憶部５６５に記憶する。受注者端末装置５１５は、公開鍵$K_{40,P}$を図４３に示す記憶部５７５に記憶する。

【０２８１】

また、受注者３３とネットワーク銀行５４０との間で所定の契約が結ばれ、ネットワーク銀行５４０は、受注者３３に対して、個人キー情報Ｚおよび個人ＩＤ情報ＩＤ２を発行する。ネットワーク銀行５４０は、個人キー情報Ｚおよび個人

ＩＤ情報ＩＤ２の対応表を図４４に示す認証装置５５０の記憶部５８５に記憶する。

【０２８２】

また、ホームゲートウェイ５１２の電源が投入されたときに電源がオンになっている端末装置511_1～511_4から内部ネットワーク１３を介してホームゲートウェイ５１２が受信した装置ＩＤ情報ID_{M1}～ID_{M4}が、図４２に示す記憶部５６５に記憶される。

【０２８３】

図４５は、トランザクション認証システム５０１の動作例を説明するための図である。

ステップＳＴ６１：

図４０に示す発注者３１は、例えばネットワーク上の商店である受注者３３に商品を発注する場合に、発注する商品名および数量などを示す発注情報ａ１と、発注者３１の個人キー情報ｋ１と、発注者３１の個人ＩＤ情報ＩＤ１とを、図示しない操作手段を操作して端末装置511_1に入力する。なお、発注情報ａ１には、受注者３３を特定する情報が含まれている。

端末装置511_1は、当該入力された発注情報ａ１と、発注者３１の個人キー情報ｋ１と、発注者３１の個人ＩＤ情報ＩＤ１と、内部メモリから読み出した装置ＩＤ情報ID_{M1}とを、内部ネットワーク１３を介して、ホームゲートウェイ５１２に送信する。

【０２８４】

ステップＳＴ６２：

図４２に示すホームゲートウェイ５１２は、発注情報ａ１と、個人キー情報ｋ１と、個人ＩＤ情報ＩＤ１と、装置ＩＤ情報ID_{M1}とを内部ネットワークＩ／Ｆ５６２で受信し、これらの全体に対して暗号化部５６３で暗号化を行う。

ホームゲートウェイ５１２は、当該暗号化した情報を格納した認証要求Ｉｎｆ１（本発明の要求）を、図４２に示す外部ネットワークＩ／Ｆ５６１から外部ネットワーク５０９を介して、図４０に示すネットワーク銀行５４０の認証装置５５０に送信する。

【０２８５】

ステップＳＴ６３：

図４４に示す認証装置５５０は、ホームゲートウェイ５１２からの認証要求Ｉｎｆ１を受信部５８１が受信すると、記憶部５８５からネットワーク銀行５４０の秘密鍵$K_{40,S}$を読み出し、復号部５８４において、当該秘密鍵$K_{40,S}$を用いて認証要求Ｉｎｆ１を復号する。

次に、認証装置５５０は、制御部５８６の制御に基づいて、上記復号した認証要求Ｉｎｆ１から個人キー情報ｋ１を削除した情報Ｉｎｆ１’とについて、記憶部５８５から読み出した自らの秘密鍵$K_{40,S}$を用いて署名情報Ａｕ１を作成する。

次に、認証装置５５０は、情報Ｉｎｆ１’および署名情報Ａｕ１を格納した要求Ｉｎｆ２を生成する。

次に、暗号化部５８３は、図４４に示す記憶部５８５から読み出した受注者３３の公開鍵$K_{33,P}$を用いて、上記生成した要求Ｉｎｆ２を暗号化した後に、送信部５８２から、外部ネットワーク５０９を介して受注者端末装置５１５に送信する。

【０２８６】

ステップＳＴ６４：

受注者端末装置５１５の復号部５７４は、認証装置５５０からの要求Ｉｎｆ２を受信部５７１が受信すると、記憶部５７５から読み出した自らの秘密鍵$K_{33,S}$を用いて、要求Ｉｎｆ２を復号する。

次に、受注者端末装置５１５の署名検証部５７７は、上記復号した要求Ｉｎｆ２に格納された署名情報Ａｕ１を、記憶部５７５から読み出した認証装置５５０の公開鍵$K_{40,P}$を用いて検証する。

【０２８７】

受注者端末装置５１５の制御部５７６は、署名検証部が上記検証の結果、署名情報Ａｕ１の正当性が認証されると、要求Ｉｎｆ２に格納された情報Ｉｎｆ１’を図４３に示す記憶部５７５に記憶する。受注者３３は、情報Ｉｎｆ１’内の発注情報ａ１に基づいて、発注者３１への商品等の発送予定などを示す受注確認情

報ｃ１を生成する。

次に、制御部５７６は、要求Ｉｎｆ２、受注確認情報ｃ１および自らの個人キー情報Ｚを格納した応答Ｉｎｆ３を生成する。

次に、受注者端末装置５１５の送信部５７２は、上記生成した応答Ｉｎｆ３を、記憶部５７５から読み出したネットワーク銀行５４０の公開鍵$K_{40,P}$を用いて暗号化部５７３で暗号化した後に、送信部５７２から、外部ネットワーク５０９を介して認証装置５５０に送信する。

受注者３３は、例えば、要求Ｉｎｆ２に格納された情報Ｉｎｆ１’内の発注情報ａ１に基づいて、発注者３１が発注した商品等を発注者３１に発送したり、発注者３１が注文したサービスを発注者３１に提供する。

【０２８８】

ステップＳＴ６５：

認証装置５５０の復号部５８４は、受注者端末装置５１５からの応答Ｉｎｆ３を受信部５８１が受信すると、記憶部５８５から読み出した自らの秘密鍵$K_{40,S}$を用いて、Ｉｎｆ３を復号し、要求Ｉｎｆ１に格納された発注情報ａ１と、当該復号されたＩｎｆ３に格納された受注者３３の個人キー情報Ｚとを用いて、所定の取り引き履歴情報を作成し、これを記憶部５８５に格納する。当該履歴情報は、ネットワーク銀行５４０が、発注者３１に対して決済を行う際に用いられる。

また、認証装置５５０の署名作成部５８７は、ステップＳＴ６４で受信した応答Ｉｎｆ３について、自らの秘密鍵$K_{40,S}$を用いて署名情報Ａｕ２を作成する。

次に、認証装置５５０の制御部５８６は、応答Ｉｎｆ３および署名情報Ａｕ２を格納した認証応答Ｉｎｆ４を作成する。

次に、認証装置５５０の暗号化部５８３は、上記作成した認証応答Ｉｎｆ４を、記憶部５８５から読み出した発注者３１の公開鍵$K_{31,P}$を用いて暗号化する。

そして、図４４に示す記憶部５８５に個人ＩＤ情報ＩＤ１と対応して記憶されているホームゲートウェイ５１２のアドレスを用いて、送信部５８２から外部ネットワーク５０９を介してホームゲートウェイ５１２に当該暗号化した応答Ｉｎｆ４を送信する。

ホームゲートウェイ５１２では、受信した認証応答Ｉｎｆ４を、図４２示す記

憶部５６５から読み出した発注者３１の秘密鍵$K_{31,S}$を用いて復号部５６４で復号する。

次に、ホームゲートウェイ５１２の署名検証部５６６は、当該復号した認証応答Ｉｎｆ４に格納された署名情報Ａｕ２を、記憶部５６５から読み出したネットワーク銀行５４０の公開鍵$K_{40,P}$を用いて検証すると共に、Ｉｎｆ４内の発注情報ａ１内に記述された装置ＩＤ情報$ＩＤ_{M1}$が図４２に示す記憶部５６５に記憶されている装置ＩＤ情報$ＩＤ_{M1}$～$ＩＤ_{M4}$の何れかと一致するか否かを判断する。当該動作例では、一致すると判断され、発注者３１と受注者３３との間の当該取り引きが正当に行われたことが確認される。

【０２８９】

ステップＳＴ６６：

ホームゲートウェイ５１２は、応答Ｉｎｆ４に含まれるＩｎｆ３を、内部ネットワーク１３を介して端末装置５１１_{1}に送信する。

端末装置５１１_{1}は、当該受信したＩｎｆ３に格納された受注確認情報ｃ１をディスプレイなどに表示する。

【０２９０】

以下、発注者３１の個人ＩＤ１および個人キーｋ１を不正に取得した図４０に示す不正者５５が自らの端末装置である不正者端末装置５５６を用いて、認証装置５５０に認証要求を送信した場合のトランザクション認証システム５０１の動作を説明する。

図４６は、トランザクション認証システム５０１の当該動作を説明するための図である。

ステップＳＴ７１：

図４０に示す不正者５５は、受注者３３に商品を発注する場合に、発注する商品名および数量などを示す発注情報ａ１と、不正に取得した発注者３１の個人キー情報ｋ１と、不正に取得した発注者３１の個人ＩＤ情報ＩＤ１とを、図示しない操作手段を操作して不正者端末装置５５６に入力する。

不正者端末装置５５６は、発注情報ａ１と、個人キー情報ｋ１と、個人ＩＤ情報ＩＤ１と、内部メモリから読み出した装置ＩＤ情報$ＩＤ_{M56}$を暗号化し、当該

暗号化した情報を格納した認証要求Ｉｎｆ１を、外部ネットワーク５０９を介して、図４０に示すネットワーク銀行５４０の認証装置５５０に送信する。

図４４に示す認証装置５５０は、不正者端末装置５５６からの認証要求Ｉｎｆ１を受信部５８１が受信すると、当該認証要求Ｉｎｆ１について、前述したステップＳＴ６２と同様の処理を行なう。

【０２９１】

ステップＳＴ７２：

ステップＳＴ７２の処理は、前述したステップＳＴ６３の処理と同じである。

【０２９２】

ステップＳＴ７３：

ステップＳＴ７３の処理は、前述したステップＳＴ６４の処理と同じである。

【０２９３】

ステップＳＴ７４：

ステップＳＴ７４の処理は、前述したステップＳＴ６５の処理と同じである。

【０２９４】

ステップＳＴ７５：

ステップＳＴ７５の処理は、前述したステップＳＴ６６の処理と同じである。

【０２９５】

このように、トランザクション認証システム５０１によれば、不正者５５が不正者端末装置５５６を用いて、認証要求Ｉｎｆ１を認証装置５５０に送信した場合でも、その応答である認証応答Ｉｎｆ４は、認証装置５５０の記憶部５８５に個人ＩＤ情報ＩＤ１と対応して記憶されているホームゲートウェイ５１２のアドレスに基づいて、ホームゲートウェイ５１２に送信される。

これにより、ホームゲートウェイ５１２において、認証応答Ｉｎｆ４に含まれる装置ＩＤ情報$ＩＤ_{M56}$が、図４２に示す記憶部５６５に記憶されている装置ＩＤ情報$ＩＤ_{M1}$～$ＩＤ_{M4}$と一致しないと判断され、発注者３１の個人ＩＤ情報ＩＤ１を用いた不正な認証要求が行なわれたことを検出できる。

そのため、トランザクション認証システム５０１によれば、他人の個人ＩＤ情報を用いた不正な取り引きを効果的に抑制できる。

【０２９６】

上述したように、トランザクション認証システム５０１によれば、電子商取引の信頼性を向上でき、当該認証機関と契約する契約者（取り引き者）の数を増やし、各契約者に課す会費などの費用を低額にでき、電子商取引をさらに普及させることが可能になる。

【０２９７】

また、トランザクション認証システム５０１によれば、例えば、図４０および図４１に示す端末装置５１１_1からの要求に応じて認証要求Ｉｎｆ１を認証装置５５０に送信した後に、端末装置５１１_1が故障した場合でも、当該認証要求Ｉｎｆ１に応じた認証応答Ｉｎｆ４に応じた処理を適切に行うことができる。

【０２９８】

また、トランザクション認証システム５０１によれば、外部ネットワーク５０９を介した通信に伴うセキュリティに関する機能をホームゲートウェイ５１２に持たせることで、端末装置５１１_1～１１_4に備えるセキュリティ機能のレベルを下げることができ、端末装置５１１_1～１１_4の構成を簡単かつ安価にできる。

【０２９９】

本発明は上述した実施形態に限定されない。

例えば、上述した実施形態では、本発明の第２の通信装置として認証処理を行う認証装置５５０を例示したが、第２の通信装置が行う処理はその他、課金処理などであってもよい。

また、上述した実施形態では、ネットワーク銀行５４０が、認証装置５５０を用いて、トランザクション（取り引き）の認証業務を行う場合を例示したが、ネットワーク銀行５４０とは別の機関が、認証装置５５０を用いてトランザクションの認証業務を行うようにしてもよい。

【０３００】

また、上述した実施形態では、端末装置５１１_1～１１_4の装置ＩＤ情報を認証装置５５０に送信した場合を例示したが、ホームゲートウェイ５１２の装置ＩＤ情報を認証装置５５０に送信するようにしてもよい。

【０３０１】

第１１実施形態

図４７は、本実施形態の認証システム８０１の全体構成図である。

図４７に示すように、認証システム８０１では、例えば、ユーザ８３１が使用する端末装置８１１と、ネットワーク銀行８２１が使用する認証装置８１３とが、インターネットなどのネットワーク（通信網）を介して接続されており、認証装置８１３がユーザ８３１の認証情報を提供する。

なお、当該ネットワークに接続されている端末装置８１１の数は任意である。

また、本実施形態では、ネットワーク銀行８２１が、認証装置８１３を使用する場合を例示するが、認証装置８１３はネットワーク銀行８２１以外の認証機関

本実施形態は、第２６～第２８の発明に対応した実施形態であり、端末装置８１１が本発明の端末装置に対応し、認証装置８１３が本発明の認証装置に対応している。

【０３０２】

以下、認証システム８０１を構成する各装置について説明する。

〔端末装置８１１〕

図４８は、端末装置８１１の機能ブロック図である。

図４８に示すように、端末装置８１１は、例えば、ユーザ８３１が使用するパーソナルコンピュータ、セット・トップ・ボックスあるいはゲーム機器などの装置であり、受信部８６１、送信部８６２、暗号化部８６３、復号部８６４、記憶部８６５、操作部８６６、表示部８６７、制御部８６８およびメモリカードアクセス部８６９を有する。

【０３０３】

受信部８６１は、ネットワークを介して認証装置８１３から情報および要求を受信する。

送信部８６２は、ネットワークを介して認証装置８１３に情報および要求を送信する。

また、受信部８６１および送信部８６２は、ネットワークを介して、その他のサーバ装置あるいは端末装置との間で情報および要求を送受信する。

【０３０４】

暗号化部８６３は、所定の暗号鍵を用いて、情報あるいは要求を暗号化する。

復号部８６４は、所定の暗号鍵を用いて、情報あるいは要求を復号する。

記憶部８６５は、認証装置８１３から受信した認証情報ＳＩＧｂなどを記憶する。ここで、認証情報ＳＩＧｂは、認証装置８１３が生成したユーザ８３１の認証情報ＳＩＧを分割して得られた情報である。

操作部８６６は、キーボードやマウスなどであり、ユーザの操作に応じた操作信号を制御部８６８やメモリカードアクセス部８６９に出力する。

表示部８６７は、制御部８６８からの表示信号に応じた画像を表示する。

制御部８６８は、端末装置８１１内の各構成要素の処理を統括的に制御する。

制御部８６８の処理については、後述する動作例で詳細に説明する。

メモリカードアクセス部８６９は、例えばユーザによって端末装置８１１に装着されたメモリカード８５０のＩＣメモリにアクセスを行う。

【０３０５】

〔認証装置８１３〕

図４９は、認証装置８１３の機能ブロック図である。

図４９に示すように、認証装置８１３は、例えば、受信部８８１、送信部８８２、暗号化部８８３、復号部８８４、記憶部８８５、操作部８８６、表示部８８７、制御部８８８およびメモリカードアクセス部８８９を有する。

ここで、受信部８８１が本発明の受信手段に対応し、送信部８８２が本発明の送信手段に対応し、記憶部８８５が本発明の記憶手段に対応し、制御部８８８が本発明の制御手段に対応し、メモリカードアクセス部８８９が本発明の書込手段に対応している。

【０３０６】

受信部８８１は、ネットワークを介して端末装置８１１から情報あるいは要求を受信する。

送信部８８２は、ネットワークを介して端末装置８１１に情報あるいは要求を送信する。

暗号化部８８３は、所定の暗号鍵を用いて、情報あるいは要求を暗号化する。

復号部８８４は、所定の暗号鍵を用いて、情報あるいは要求を復号する。

記憶部８８５は、登録（契約）したユーザの個人情報、個人ＩＤ情報、後述するようにして生成された認証情報ＳＩＧ，ＳＩＧａ，ＳＩＧｂ、並びに認証情報ＳＩＧａのダウンロード先の装置ＩＤ情報などを記憶する。

ここで、認証情報ＳＩＧが本発明の認証情報に対応し、認証情報ＳＩＧａが本発明の第１の認証情報に対応し、認証情報ＳＩＧｂが本発明の第２の認証情報に対応している。

【０３０７】

操作部８８６は、キーボードおよびマウスなどであり、ユーザの操作に応じた操作信号を制御部８８８に出力する。

表示部８８７は、制御部８８８からの表示信号に応じた画像を表示する。

制御部８８８は、認証装置８１３内の各構成要素の処理を統括的に制御する。

制御部８８８の処理については、後述する動作例で詳細に説明する。

メモリカードアクセス部８８９は、登録したユーザに発行するメモリカード８５０のＩＣメモリに、当該ユーザに対応する認証情報ＳＩＧｂを書き込む。

【０３０８】

以下、認証システム８０１の動作例を説明する。

〔第１の動作例〕

ここでは、ネットワーク銀行８２１が認証情報ＳＩＧを分割して得られた認証情報ＳＩＧｂを記憶されたメモリカード８５０を作成し、これをユーザ８３１に送付するまでの動作例を説明する。

図５０は、当該動作例を説明するためのフローチャートである。

ステップＳＴ１：

ユーザ８３１が図４８に示す端末装置８１１の操作部８６６を操作して、登録要求と共に、自らの個人情報、並びに認証情報ＳＩＧａのダウンロード先（送信先）として指定する単数または複数の端末装置（本実施形態では、端末装置８１１）の装置ＩＤ情報を入力する。これにより、当該入力された情報を含む登録要求が、ネットワークを介して端末装置８１１の送信部８６２から認証装置８１３に送信される。

【０３０９】

ステップＳＴ２：

認証装置８１３は、ステップＳＴ１で端末装置８１１から受信部８８１が受信した登録要求に応じて、ユーザ８３１に固有の個人ＩＤ情報を発行し、当該個人ＩＤ情報と、登録要求に含まれる個人情報およびダウンロード先の情報とを図４９に示す記憶部８８５に書き込む。

【０３１０】

ステップＳＴ３：

認証装置８１３は、登録要求に応じて、公開鍵暗号化方式（ＰＫＩ:Public Key Infrastructure）を用いて、ユーザ８３１の認証情報ＳＩＧを生成する。

当該認証情報ＳＩＧは、ユーザ８３１の個人認証に用いられる情報である。

【０３１１】

ステップＳＴ４：

認証装置８１３は、ステップＳＴ３で生成した認証情報ＳＩＧを、認証情報ＳＩＧａと認証情報ＳＩＧｂとに分割する。

【０３１２】

ステップＳＴ５：

認証装置８１３は、端末装置８１１の個人ＩＤ情報と関連付けて、認証情報ＳＩＧ，ＳＩＧａ，ＳＩＧｂを記憶部８８５に書き込む。

【０３１３】

ステップＳＴ６：

認証装置８１３のメモリカードアクセス部８８９は、ユーザ８３１に発行するメモリカード８５０のＩＣメモリに、ユーザ８３１の個人ＩＤ情報および認証情報ＳＩＧｂを書き込む。

このとき、認証情報ＳＩＧｂは、図４９に示す暗号化部８８３で暗号化された後に、メモリカード８５０のＩＣメモリに書き込まれてもよい。

【０３１４】

ステップＳＴ７：

ネットワーク銀行８２１の担当者は、ステップＳＴ６の処理を経たメモリカー

ド８５０を郵便などのオフラインでユーザ８３１に送付する。

【０３１５】

ユーザ８３１は、ネットワーク銀行８２１が送付したメモリカード８５０を受け取る。

【０３１６】

〔第２の動作例〕

当該動作例では、ユーザ８３１がメモリカード８５０を用いて、端末装置８１１で認証情報を得るときの動作例を説明する。

図５１および図５２は、当該動作例を説明するためのフローチャートである。

ステップＳＴ１１：

ユーザ８３１は、メモリカード８５０を端末装置８１１のメモリカードアクセス部８６９に装着する。

【０３１７】

ステップＳＴ１２：

ユーザ８３１は、図４８に示す操作部８６６を操作して、認証情報要求と共に、自らの個人ＩＤ情報と、ダウンロード先としての端末装置８１１の装置ＩＤ情報とを入力する。

これにより、当該入力された情報を含む認証情報要求がネットワークを介して端末装置８１１の送信部８６２から認証装置８１３に送信される。

【０３１８】

ステップＳＴ１３：

認証装置８１３の受信部８８１は、ステップＳＴ１２で端末装置８１１が送信した認証情報要求を受信する。

【０３１９】

ステップＳＴ１４：

認証装置８１３の制御部８８８は、ステップＳＴ１３で受信部８８１が受信した認証情報要求に含まれる個人ＩＤ情報に対応するダウンロード先の情報を図４９に示す記憶部８８５から読み出し、当該読み出したダウンロード先の情報内に、認証情報要求に含まれるダウンロード先の情報に存在するか否かを判断し、存

在すると判断した場合には認証情報要求が正当であるとし、存在しないと判断した場合には認証情報要求が不当であると判断する。

【０３２０】

ステップＳＴ１５：

認証装置８１３の制御部８８８は、認証情報要求が正当であると判断すると、認証情報要求に含まれる個人ＩＤ情報に対応する認証情報ＳＩＧａを記憶部８８５から読み出し、当該読み出した認証情報ＳＩＧａを、指定された装置ＩＤ情報によって特定される端末装置（本実施形態では、端末装置８１１）に送信部８８２を介して送信する。

【０３２１】

ステップＳＴ１６：

一方、認証装置８１３の制御部８８８は、認証情報要求が不正であると判断すると、認証情報要求に含まれる個人ＩＤ情報に対応するダウンロード先の装置ＩＤ情報を記憶部８８５から読み出し、当該読み出した装置ＩＤ情報によって特定される装置に、送信部８８２を介して、メモリカード８５０が不正に用いられた旨を示す通知を送信する。

【０３２２】

ステップＳＴ１７：

端末装置８１１の受信部８６１は、認証装置８１３から認証情報ＳＩＧａを受信する。

【０３２３】

ステップＳＴ１８：

端末装置８１１の制御部８６８は、ステップＳＴ１４で受信部８６１が受信した認証情報ＳＩＧａと、メモリカード８５０に記憶されている認証情報ＳＩＧｂとが対応しているか否かを判断する。

【０３２４】

ステップＳＴ１９：

端末装置８１１の制御部８６８は、ステップＳＴ１８で対応していると判断すると、ステップＳＴ１７で受信部８６１が受信した認証情報ＳＩＧａを記憶部８

６５に書き込む。

これにより、端末装置８１１の制御部８６８は、記憶部８６５に記憶された認証情報ＳＩＧａおよびＳＩＧｂを用いて認証情報ＳＩＧを復元する。

【０３２５】

ステップＳＴ２０：

端末装置８１１の制御部８６８は、ステップＳＴ１６で対応していないと判断すると、その旨を示す通知を、ネットワークを介して、送信部８６２から認証装置８１３に送信する。

【０３２６】

ステップＳＴ２１：

認証装置８１３の受信部８８１は、端末装置８１１から通知を受信する。

【０３２７】

ステップＳＴ２２：

認証装置８１３は、対応する正規に登録されたユーザの端末装置にメモリカード８５０が不正使用された旨を示す通知を送信部８８２から、ネットワークを介して送信する。

【０３２８】

以上説明したように、認証システム８０１によれば、メモリカード８５０には、認証情報ＳＩＧの一部の認証情報ＳＩＧｂのみを記憶し、端末装置８１１からの認証情報要求に応じて、認証装置８１３において、ユーザの正当性を検証した後に、残りの認証情報ＳＩＧａを認証装置８１３から端末装置８１１に送信し、端末装置８１１内で認証情報ＳＩＧを復元するするため、メモリカード８５０を盗難されたり、紛失した場合でも、不正なユーザは、メモリカード８５０だけでは認証情報ＳＩＧを得ることができない。そのため、メモリカード８５０を用いた、なりすましなどの不正利用を防止できる。

【０３２９】

本発明は上述した実施形態には限定されない。

上述した実施形態では、ダウンロード先として、認証情報要求を送信する端末装置８１１を指定した場合を例示したが、その他の端末装置を指定することもで

きる。これにより、家庭内などに複数の端末装置がある場合に、一の端末装置にメモリカード８５０を装着すれば、他の端末装置でも、メモリカード８５０のユーザの認証情報を得ることができる。

【０３３０】

【発明の効果】

以上説明したように本発明によれば、ネットワークを介した電子商取引の安全性を高めことができる認証装置、処理装置、認証システムおよびその方法を提供できる。

また、本発明によれば、第１の取り引き者の個人キー情報が第２の取り引き者に提供されないようにすることで、個人キー情報を用いた不正行為を効果的に抑制する認証装置、処理装置、認証システムおよびその方法を提供できる。

【０３３１】

また、本発明によれば、不正に取得した他人の識別情報（個人ＩＤ情報）に基づいて不正な認証手続が行われることを回避する認証装置、処理装置、認証システムおよびその方法を提供できる。

【０３３２】

また、本発明によれば、例えば異なる認証機関と契約した複数の取り引き者間での取り引きの認証を、取り引き者の個人情報を他の認証機関に提供することなく、高い信頼性で行うことができる認証装置、認証システムおよびその方法を提供できる。

【０３３３】

また、本発明によれば、不正に取得した他人の識別情報（個人ＩＤ情報）に基づいて不正な手続が行われることを回避する通信装置、通信システムおよびその方法を提供できる。

【０３３４】

また、本発明によれば、不正に取得した他人の識別情報（個人ＩＤ情報）に基づいて不正な認証手続が行われることを回避する通信制御装置、通信システムおよびその方法を提供できる。

また、本発明によれば、複数の通信装置を用いてネットワークを介した電子商

取引などを行う場合に、当該電子商取引に必要な機能の割り当て、並びに通信履歴の管理を効率的に行うことができる通信制御装置、通信システムおよびその方法を提供できる。

【０３３５】

また、本発明によれば、情報を高い秘匿性を保ちながら記録媒体に記録できる情報記録方法およびその装置と、そのような形態で情報が記録された記録媒体とを提供できる。

また、本発明によれば、上述したような情報記録方法およびその装置によって記録媒体に記録された情報を適切に復元できる情報復元方法およびその装置を提供できる。

【０３３６】

また、本発明によれば、個人認証機能を持つ携帯型メモリ装置を用いて認証を行う場合に、煩雑な手続きを行うことなく、その安全性を高めることができる。

【図面の簡単な説明】

【図１】

図１は、本発明の第１実施形態に係わるトランザクション認証システムの全体構成図である。

【図２】

図２は、図１に示す発注者端末装置の機能ブロック図である。

【図３】

図３は、図１に示す認証装置の機能ブロック図である。

【図４】

図４は、図１に示す受注者端末装置の機能ブロック図である。

【図５】

図５は、図１に示すトランザクション認証システムの動作を説明するための図である。

【図６】

図６は、本発明の第２実施形態に係わるトランザクション認証システムの全体構成図である。

【図７】

図７は、図６に示す発注者端末装置の機能ブロック図である。

【図８】

図８は、図６に示す認証装置の機能ブロック図である。

【図９】

図９は、図６に示す受注者端末装置の機能ブロック図である。

【図１０】

図１０は、図６に示すトランザクション認証システムの動作を説明するための図である。

【図１１】

図１１は、本発明の第３実施形態のトランザクション認証システムの全体構成図である。

【図１２】

図１２は、図１１に示す発注者端末装置の構成図である。

【図１３】

図１３は、図１１に示す受注者端末装置の構成図である。

【図１４】

図１４は、図１１に示す認証装置（Ａ）の構成図である。

【図１５】

図１５は、図１１に示す認証装置（Ｂ）の構成図である。

【図１６】

図１６は、図１１に示すトランザクション認証システムの動作例を説明するための情報の流れを示す図である。

【図１７】

図１７は、本発明の第４実施形態の情報記録装置の構成図である。

【図１８】

図１８は、図１７に示す情報記録装置における処理の情報の流れを説明するための図である。

【図１９】

図１９は、図１７に示す情報記録装置の処理のフローチャートである。

【図２０】

図２０は、本発明の第５実施形態の情報復元装置の構成図である。

【図２１】

図２１は、図２０に示す情報復元装置における処理の情報の流れを説明するための図である。

【図２２】

図２２は、図２０に示す情報復元装置の処理のフローチャートである。

【図２３】

図２３は、本発明の第６実施形態の情報記録装置の構成図である。

【図２４】

図２４は、図２３に示す情報記録装置における処理の情報の流れを説明するための図である。

【図２５】

図２５は、図２３に示す情報記録装置の処理のフローチャートである。

【図２６】

図２６は、本発明の第７実施形態の情報復元装置の構成図である。

【図２７】

図２７は、図２６に示す情報復元装置における処理の情報の流れを説明するための図である。

【図２８】

図２８は、図２６に示す情報復元装置の処理のフローチャートである。

【図２９】

図２９は、本発明の第８実施形態に係わるトランザクション認証システムの全体構成図である。

【図３０】

図３０は、図２９に示す発注者端末装置の構成図である。

【図３１】

図３１は、図２９に示す受注者端末装置の構成図である。

【図３２】

図３２は、図２９に示す認証装置の構成図である。

【図３３】

図３３は、図２９に示すトランザクション認証システムの動作例を説明するための情報の流れを示す図である。

【図３４】

図３４は、本発明の第９実施形態のトランザクション認証システムの全体構成図である。

【図３５】

図３５は、図３４に示す発注者端末装置の構成図である。

【図３６】

図３６は、図３４に示す受注者端末装置の構成図である。

【図３７】

図３７は、図３４に示す認証装置の構成図である。

【図３８】

図３８は、発注者が認証装置に認証要求を行なった場合のトランザクション認証システムの動作のフローチャートである。

【図３９】

図３９は、不正者が認証装置に認証要求を行なった場合のトランザクション認証システムの動作のフローチャートである。

【図４０】

図４０は、本発明の第１０実施形態のトランザクション認証システムの全体構成図である。

【図４１】

図４１は、図４０に示すホームネットワークシステムを説明するための図である。

【図４２】

図４２は、図４１に示すホームゲートウェイの構成図である。

【図４３】

図４３は、図４０に示す受注者端末装置の構成図である。

【図４４】

図４４は、図４０に示す認証装置の構成図である。

【図４５】

図４５は、正当者が認証要求を出した場合の図４０に示すトランザクション認証システムの動作例を説明するための情報の流れを示す図である。

【図４６】

図４６は、不正者が認証要求を出した場合の図４０に示すトランザクション認証システムの動作例を説明するための情報の流れを示す図である。

【図４７】

図４７は、本発明の第１１実施形態の認証システムの全体構成図である。

【図４８】

図４８は、図４７に示す端末装置の機能ブロック図である。

【図４９】

図４９は、図４７に示す認証装置の機能ブロック図である。

【図５０】

図５０は、図４７に示す認証システムにおいて、ネットワーク銀行が認証情報の一部が記憶されたメモリカードを作成し、これをユーザに送付するまでの動作例を説明するためのフローチャートである。

【図５１】

図５１は、図４７に示す認証システムにおいて、ユーザがメモリカードを用いて、端末装置で認証情報を得るときの動作例を説明するためのフローチャートである。

【図５２】

図５２は、図４７に示す認証システムにおいて、ユーザがメモリカードを用いて、端末装置で認証情報を得るときの動作例を説明するためのフローチャートである。

【符号の説明】

１…トランザクション認証システム、１１…発注者端末装置、１１ａ…認証要

求入力部、１１ｂ…認証要求送信部、１１ｃ…認証応答受信部、１１ｄ…認証要求暗号化部、１１ｅ…認証応答復号部、１２…生体認証装置、１３…認証装置、１３ａ…認証要求受信部、１３ｂ…発注者認証部、１３ｃ…要求生成部、１３ｄ…要求送信部、１３ｅ…応答受信部、１３ｆ…受注者認証部、１３ｇ…認証応答生成部、１３ｈ…認証応答暗号化部、１３ｉ…認証応答送信部、１３ｊ…要求暗号化部、１３ｋ…応答復号部、１３１…認証要求復号部、１４…認証履歴格納装置、１５…受注者端末装置、１５ａ…認証要求受信部、１５ｂ…要求復号部、１５ｃ…応答入力部、１５ｄ…応答生成部、１５ｅ…応答暗号化部、１５ｆ…応答送信部、

１０１…トランザクション認証システム、１１…発注者端末装置、１１ａ…認証要求入力部、１１ｂ…認証要求送信部、１１ｃ…認証応答受信部、１１ｄ…認証要求暗号化部、１１ｅ…認証応答復号部、１２…生体認証装置、１３…認証装置、１１３ａ…認証要求受信部、１１３ｂ…発注者認証部、１１３ｃ…要求生成部、１１３ｄ…要求送信部、１１３ｅ…応答受信部、１１３ｆ…受注者認証部、１１３ｇ…認証応答生成部、１１３ｈ…認証応答暗号化部、１１３ｉ…認証応答送信部、１１３ｊ…要求暗号化部、１１３ｋ…応答復号部、１１３１…認証要求復号部、１４…認証履歴格納装置、１５…受注者端末装置、１１５ａ…認証要求受信部、１１５ｂ…要求復号部、１１５ｃ…応答入力部、１１５ｄ…応答生成部、１１５ｅ…応答暗号化部、１１５ｆ…応答送信部

２０１…トランザクション認証システム、２１１…発注者端末装置、２１５…受注者端末装置、３１…発注者、３３…受注者、２４０…ネットワーク銀行、２５０…認証装置、２６１，２７１，２８１…受信部、２６２，２７２，２８２…送信部、２６３，２７３，２８３…暗号化部、２６４，２７４，２８４…復号部、２６５，２７５，２８５…記憶部、２６６，２７６，２８６…制御部、２６７，２７７…署名検証部、，２８７…署名作成部、２８８…課金処理部、ａ１…発注情報、ｋ１…発注者３１の個人キー情報ｋ１、ＩＤ１…発注者３１の個人ＩＤ情報、ID_M…装置ＩＤ情報、Ａｕ１，Ａｕ２…認証装置の署名情報、Ｚ…受注者の個人キー情報、Ｉｎｆ１…認証要求、Ｉｎｆ４…認証応答

３０１…トランザクション認証システム、３１１…発注者端末装置、３１５…

受注者端末装置、３４０，３４１…ネットワーク銀行、３５０，３５１…認証装置、３６１，３７１，３８１，３９１…受信部、３６２，３７２，３８２，３９２…送信部、３６３，３７３，３８３，３９３…暗号化部、３６４，３７４，３８４，３９４…復号部、３６５，３７５，３８５，３９５…記憶部、３６６，３７６，３８６，３９６…制御部、３６７，３７７…署名検証部、３８７，３９７…署名作成部、３８８，３９８…課金処理部

ａ１…発注情報、ｋ１…発注者３１の個人キー情報ｋ１、ＩＤ１…発注者３１の個人ＩＤ情報、ｂ１…受注者を特定する情報、Ａｕ－Ｂ…認証装置５１の署名情報、Ａｕ－Ａ１，Ａｕ－Ａ２…認証装置５０の署名情報、Ｚ…受注者の個人キー情報

４０１…トランザクション認証システム、４１１…発注者端末装置、４１５…受注者端末装置、４４０…ネットワーク銀行、４５０…認証装置、４６１，４７１，４８１…受信部、４６２，４７２，４８２…送信部、４６３，４７３，４８３…暗号化部、４６４，４７４，４８４…復号部、４６５，４７５，４８５…記憶部、４６６，４７６，４８６…制御部、４６７，４７７…署名検証部、，４８７…署名作成部、４８８…課金処理部、ａ１…発注情報、ｋ１…発注者３１の個人キー情報ｋ１、ＩＤ１…発注者３１の個人ＩＤ情報、ＩＤ＿Ｎ…ネットワークＩＤ、Ａｕ１，Ａｕ２…認証装置の署名情報、Ｚ…受注者の個人キー情報、Ｉｎｆ１…認証要求、Ｉｎｆ４…認証応答

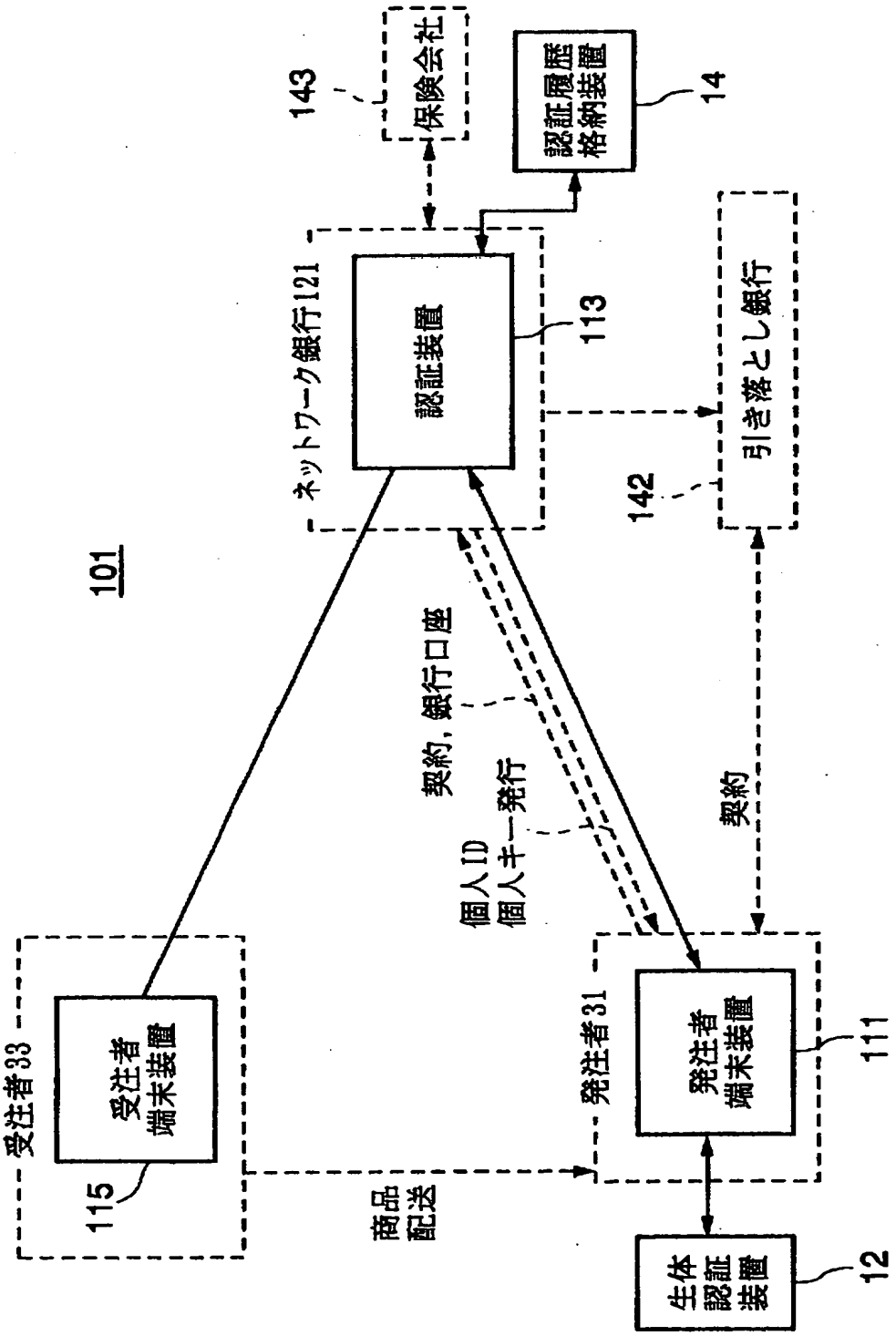
５０１…トランザクション認証システム、５１１…発注者端末装置、５１５…受注者端末装置、５４０…ネットワーク銀行、５５０…認証装置、５６１…外部ネットワークＩ／Ｆ、５６２…内部ネットワークＩ／Ｆ、５７１，５８１…受信部、５７２，５８２…送信部、５６３，５７３，５８３…暗号化部、５６４，５７４，５８４…復号部、５６５，５７５，５８５…記憶部、５６６，５７６，５８６…制御部、５６７，５７７…署名検証部、，５８７…署名作成部、５８８…課金処理部、ａ１…発注情報、ｋ１…発注者３１の個人キー情報ｋ１、ＩＤ１…発注者３１の個人ＩＤ情報、ID_{M1}，ID_{M2}，ID_{M3}，ID_{M4}，ID_{M56}…装置ＩＤ情報、Ａｕ１，Ａｕ２…認証装置の署名情報、Ｚ…受注者の個人キー情報、Ｉｎｆ１…認証要求、Ｉｎｆ４…認証応答

６０１…情報記録装置、６１０…読み出し回路、６１１…暗号化回路、６１２…情報分割回路、６１３，６１４…書き込み回路、６１５，６１６，６１７…記録媒体、６２０，６２１…読み出し回路、６２２…情報合成回路、６２３…復号回路、６２４…書き込み回路、６３１…情報復元装置、６４１…情報記録装置、６５０…読み出し回路、６５１…情報分割回路、６５２，６５３…暗号化回路、６５４，６５５…書き込み回路、６６１…情報復号装置、６７０，６７１…読み出し回路、６７２，６７３…復号回路、６７４…情報合成回路、６７５…書き込み回路

８０１…認証システム、８１１…端末装置、８１３…認証装置、８２１…ネットワーク銀行、８３１…ユーザ、８６１，８８１…受信部、８６２，８８２点送信部、８６３，８８３…暗号化部、８６４，８８４…復号部、８６５，８８５…記憶部、８６６，８８６…記憶部、８６７，８８７…表示部、８６８，８８８…制御部、８６９，８８９…メモリカードアクセス部

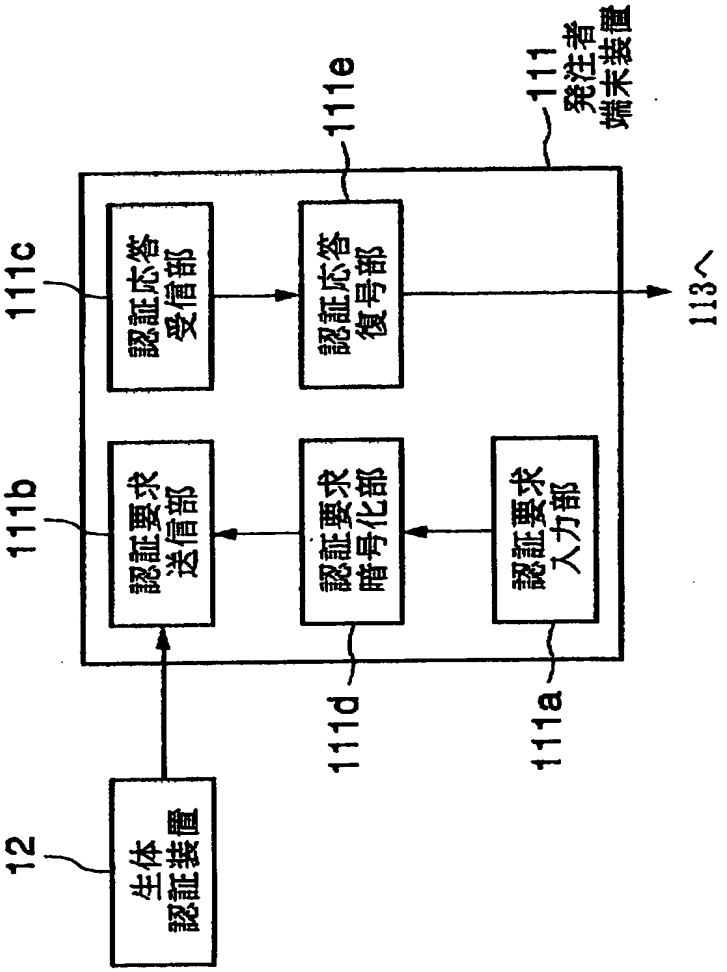
【書類名】　図面

【図１】

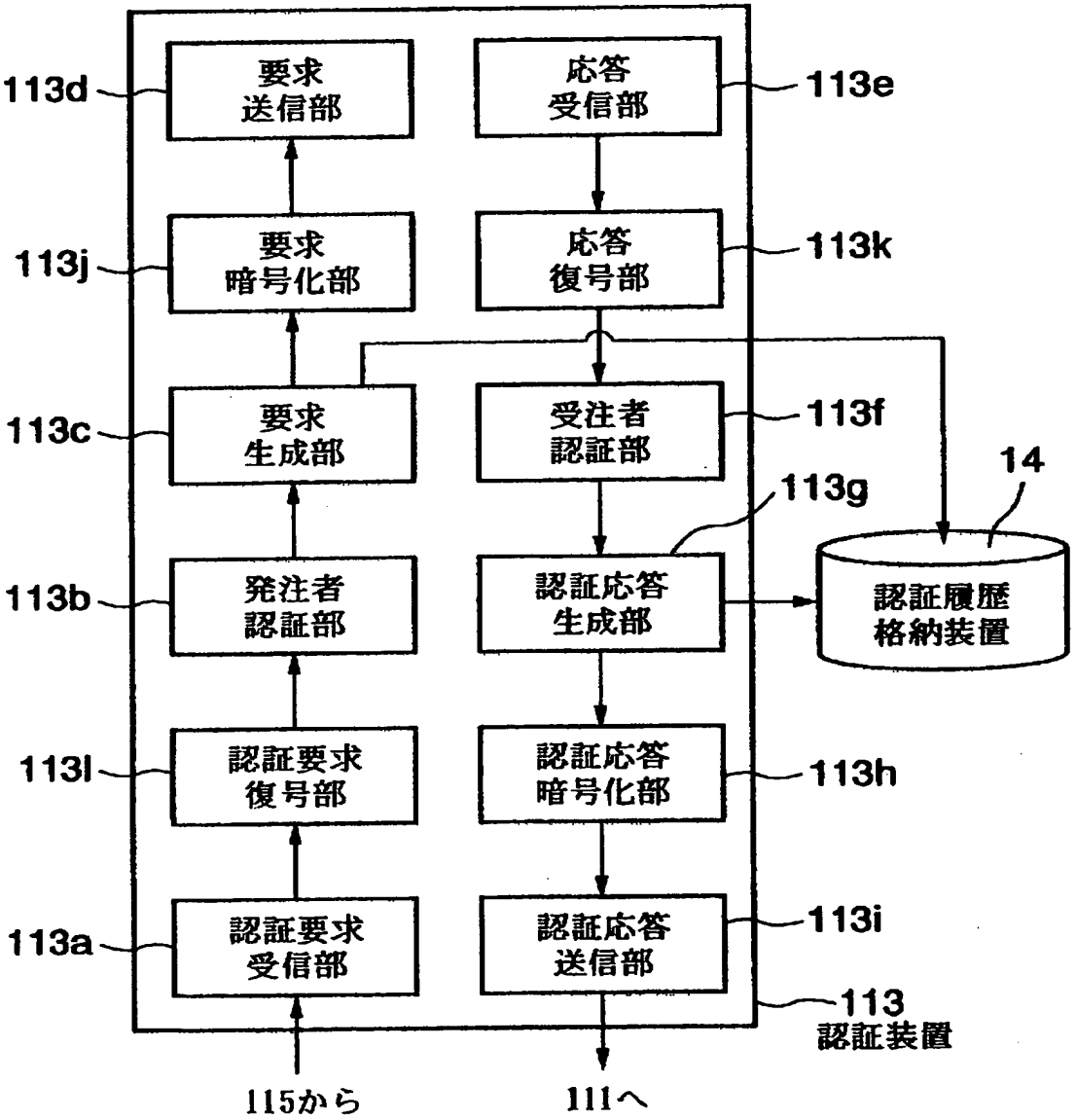


出証特２００１－３０１５２０２

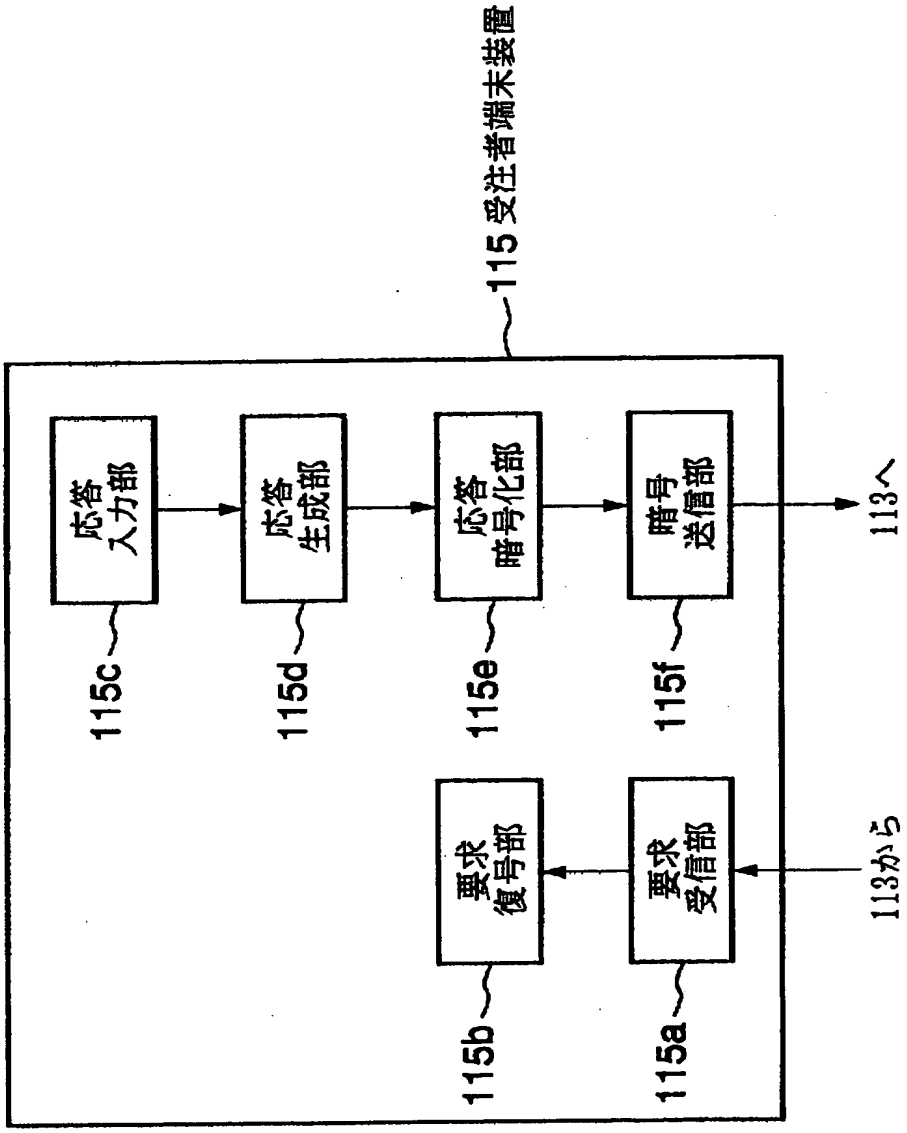
【図２】


111
発注者
端末装置
111e
111c
認証応答
受信部
認証応答
復号部
113へ
111b
認証要求
送信部
認証要求
暗号化部
認証要求
入力部
111d
111a
12
生体
認証装置

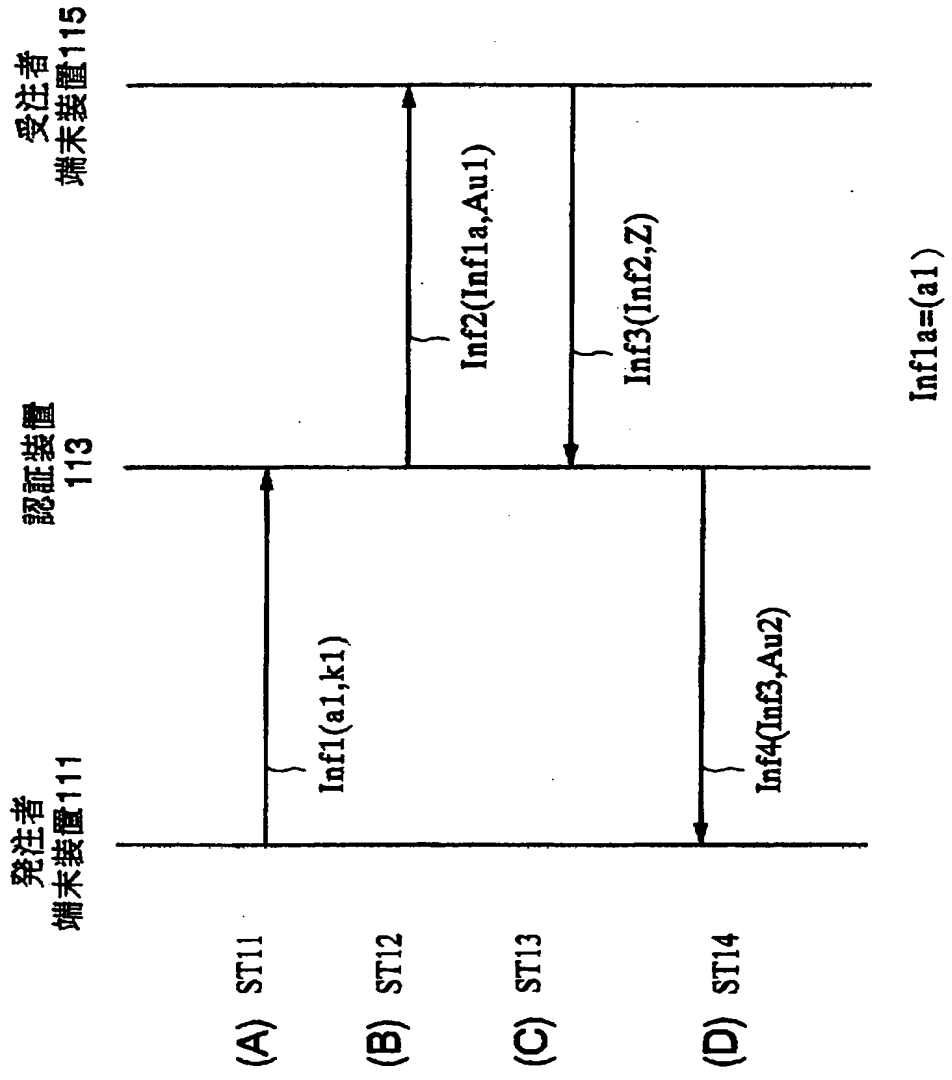
【図３】


113d
要求
送信部
応答
受信部
113e
113j
要求
暗号化部
応答
復号部
113k
113c
要求
生成部
受注者
認証部
113f
14
113g
113b
発注者
認証部
認証応答
生成部
認証履歴
格納装置
113l
認証要求
復号部
認証応答
暗号化部
113h
113a
認証要求
受信部
認証応答
送信部
113i
113
認証装置
115から
111へ

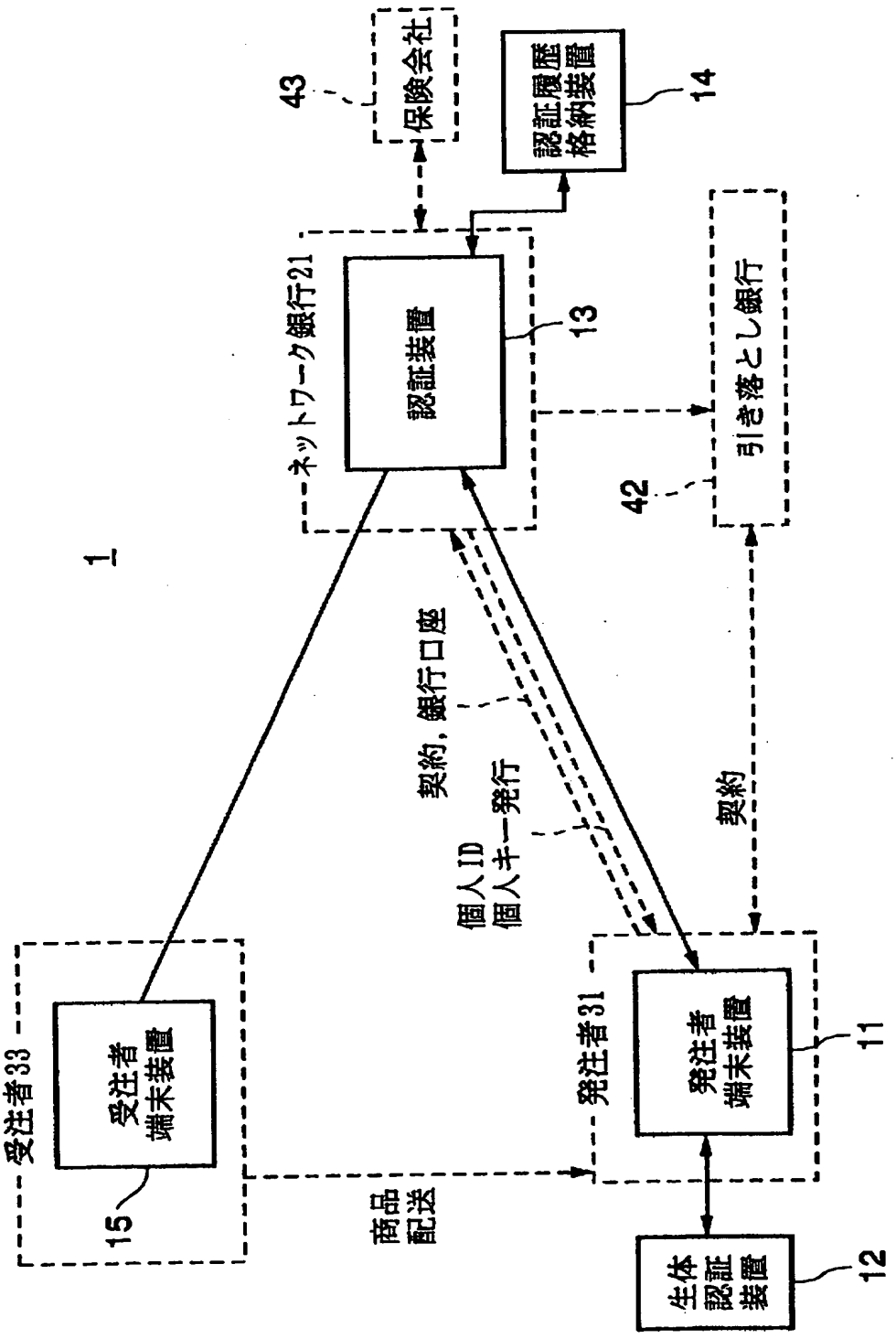
【図４】


115 受注者端末装置
応答入力部
応答生成部
応答暗号化部
暗号送信部
113へ
115c
115d
115e
115f
要求復号部
要求受信部
113から
115b
115a

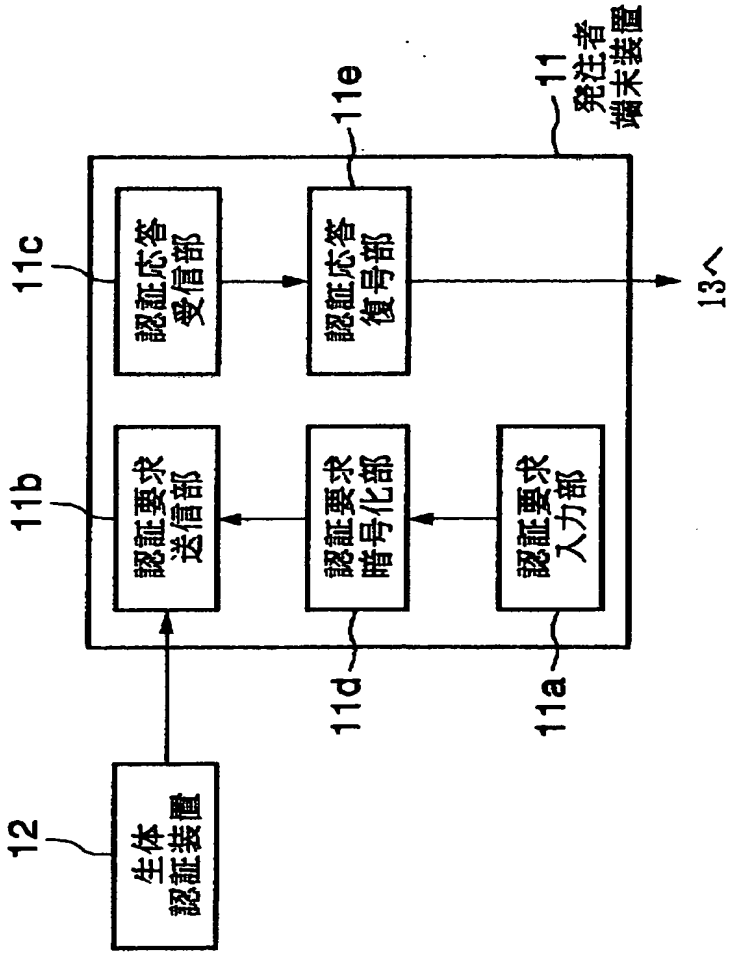
【図５】


受注者
端末装置115
認証装置
113
発注者
端末装置111
Inf1(a1,k1)
Inf2(Inf1a,Au1)
Inf3(Inf2,Z)
Inf4(Inf3,Au2)
Inf1a=(a1)
(A) ST11
(B) ST12
(C) ST13
(D) ST14

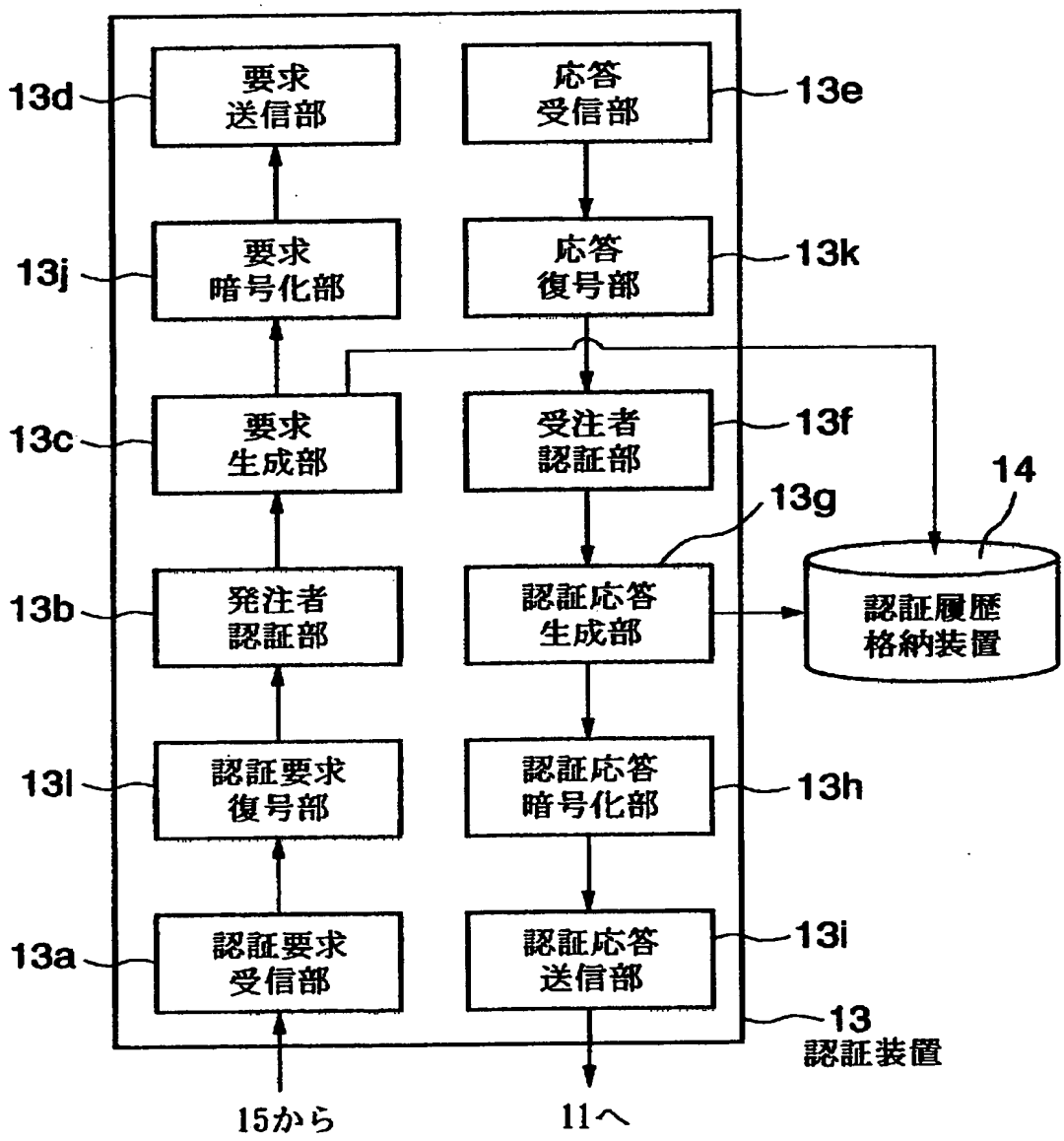
【図６】


1
ネットワーク銀行21
認証装置
13
保険会社
43
認証履歴
格納装置
14
引き落とし銀行
42
契約，銀行口座
個人ID
個人キー発行
契約
受注者33
受注者
端末装置
15
商品
配送
発注者31
発注者
端末装置
11
生体
認証
装置
12

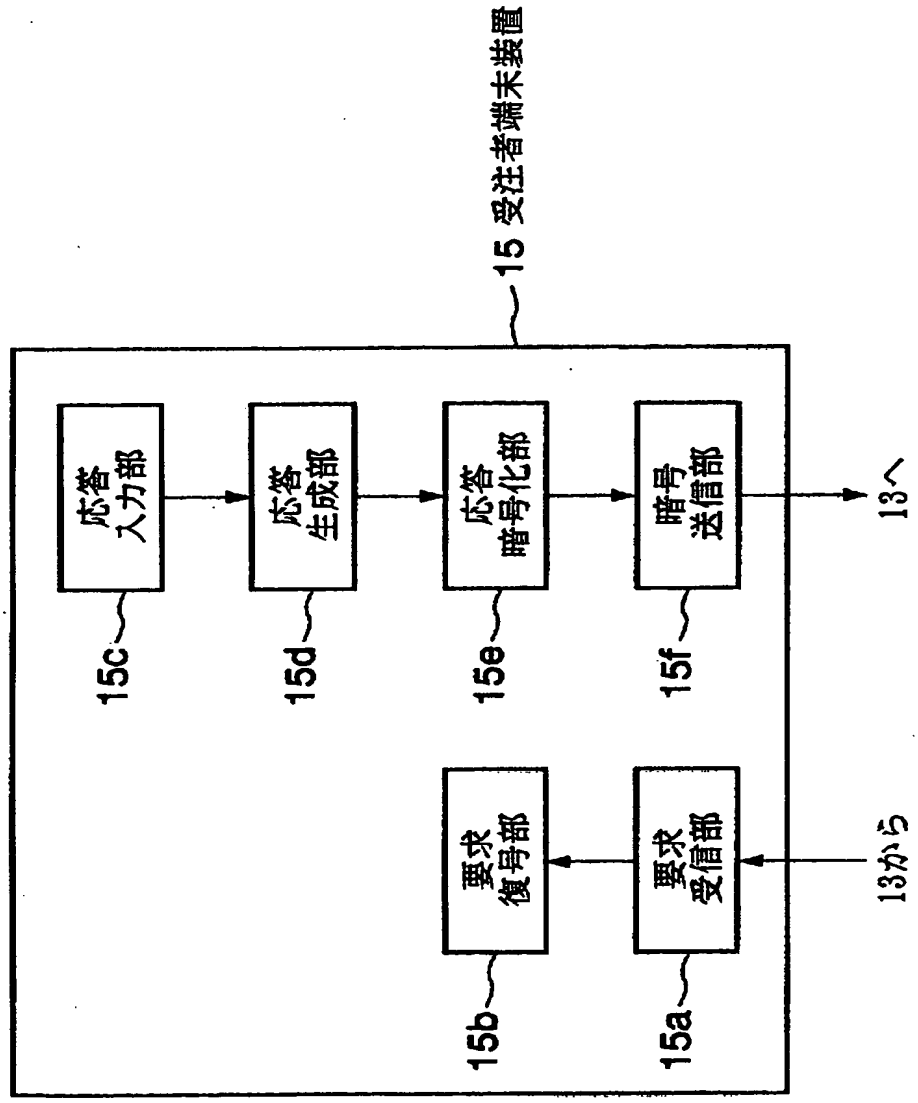
【図７】


11
発注者
端末装置
11e
11c
認証応答
受信部
認証応答
復号部
13へ
11b
認証要求
送信部
認証要求
暗号化部
認証要求
入力部
11d
11a
12
生体
認証装置

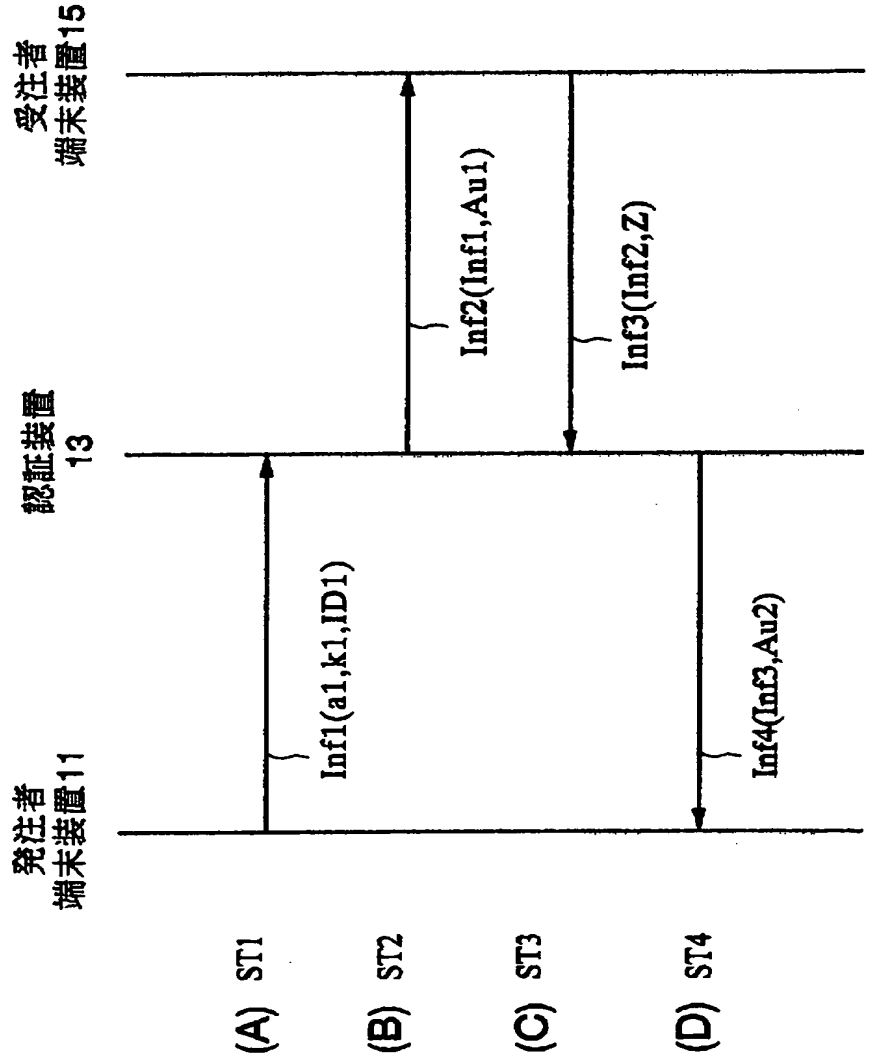
【図８】


13d
要求
送信部
応答
受信部
13e
13j
要求
暗号化部
応答
復号部
13k
13c
要求
生成部
受注者
認証部
13f
14
13g
13b
発注者
認証部
認証応答
生成部
認証履歴
格納装置
13l
認証要求
復号部
認証応答
暗号化部
13h
13a
認証要求
受信部
認証応答
送信部
13i
13
認証装置
15から
11へ

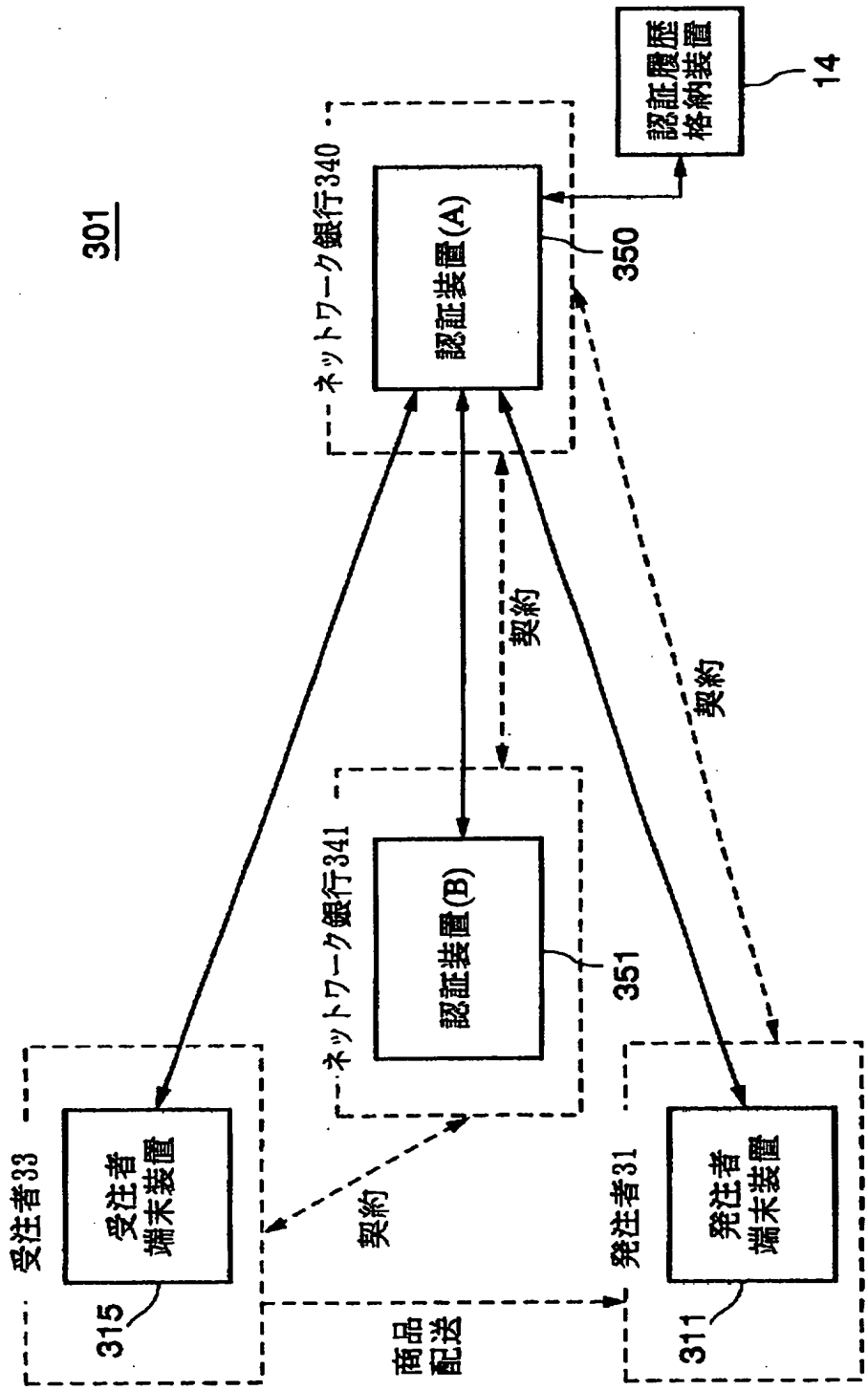
【図９】


15 受注者端末装置
応答入力部
応答生成部
応答暗号化部
暗号送信部
13へ
15c
15d
15e
15f
要求復号部
要求受信部
13から
15b
15a

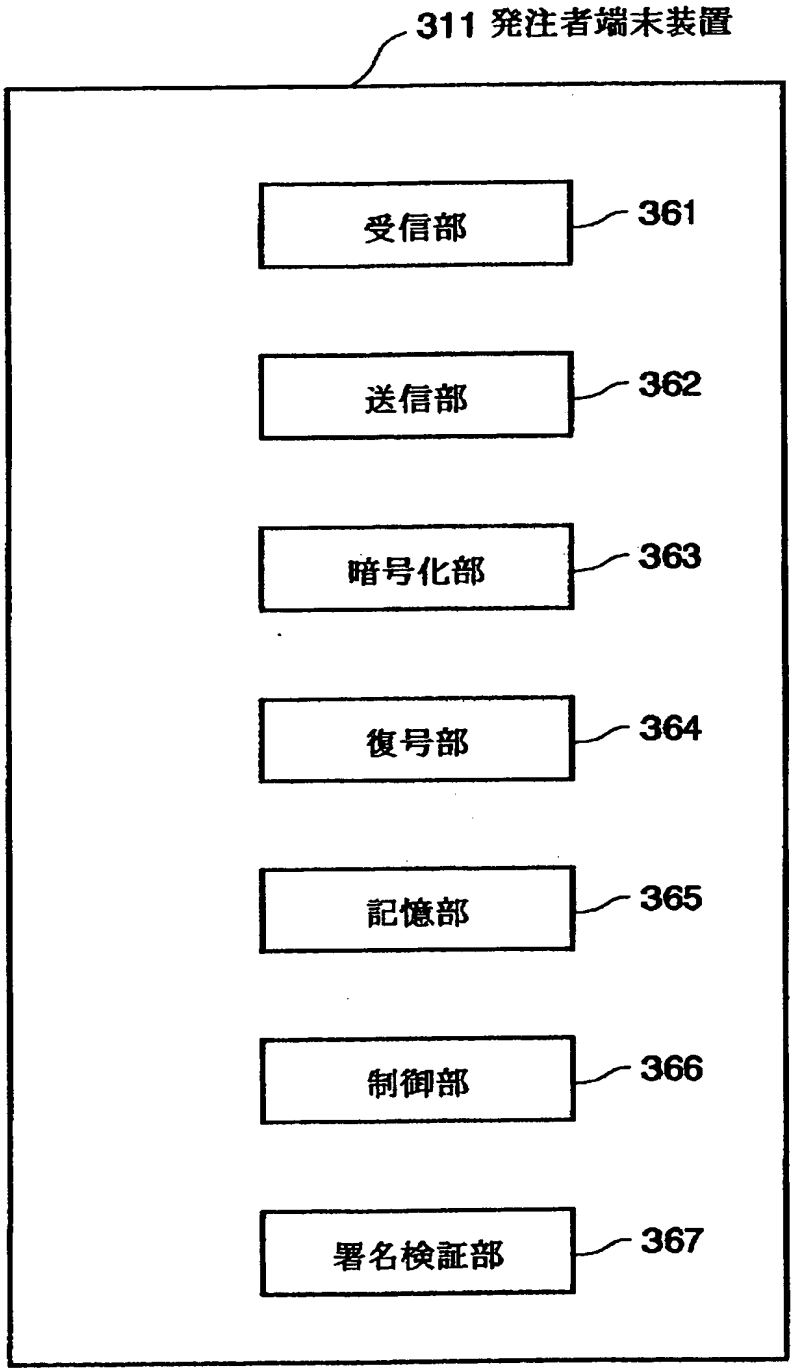
【図１０】


受注者
端末装置15
認証装置
13
発注者
端末装置11
Inf1(a1,k1,ID1)
Inf2(Inf1,Au1)
Inf3(Inf2,Z)
Inf4(Inf3,Au2)
(A) ST1
(B) ST2
(C) ST3
(D) ST4

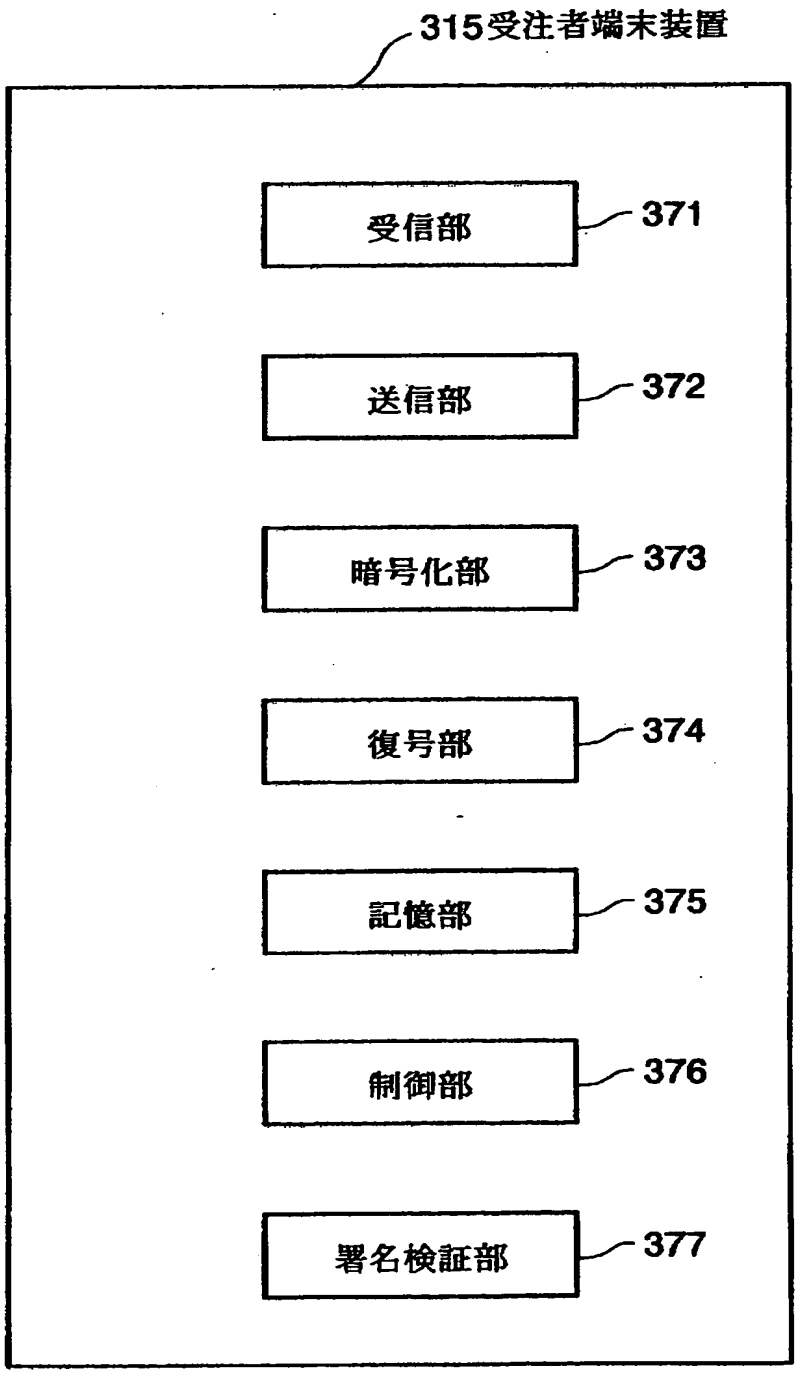
【図１１】


301
ネットワーク銀行340
認証装置(A)
認証履歴格納装置
14
350
契約
契約
ネットワーク銀行341
認証装置(B)
351
受注者33
受注者端末装置
315
契約
発注者31
発注者端末装置
311
商品配送

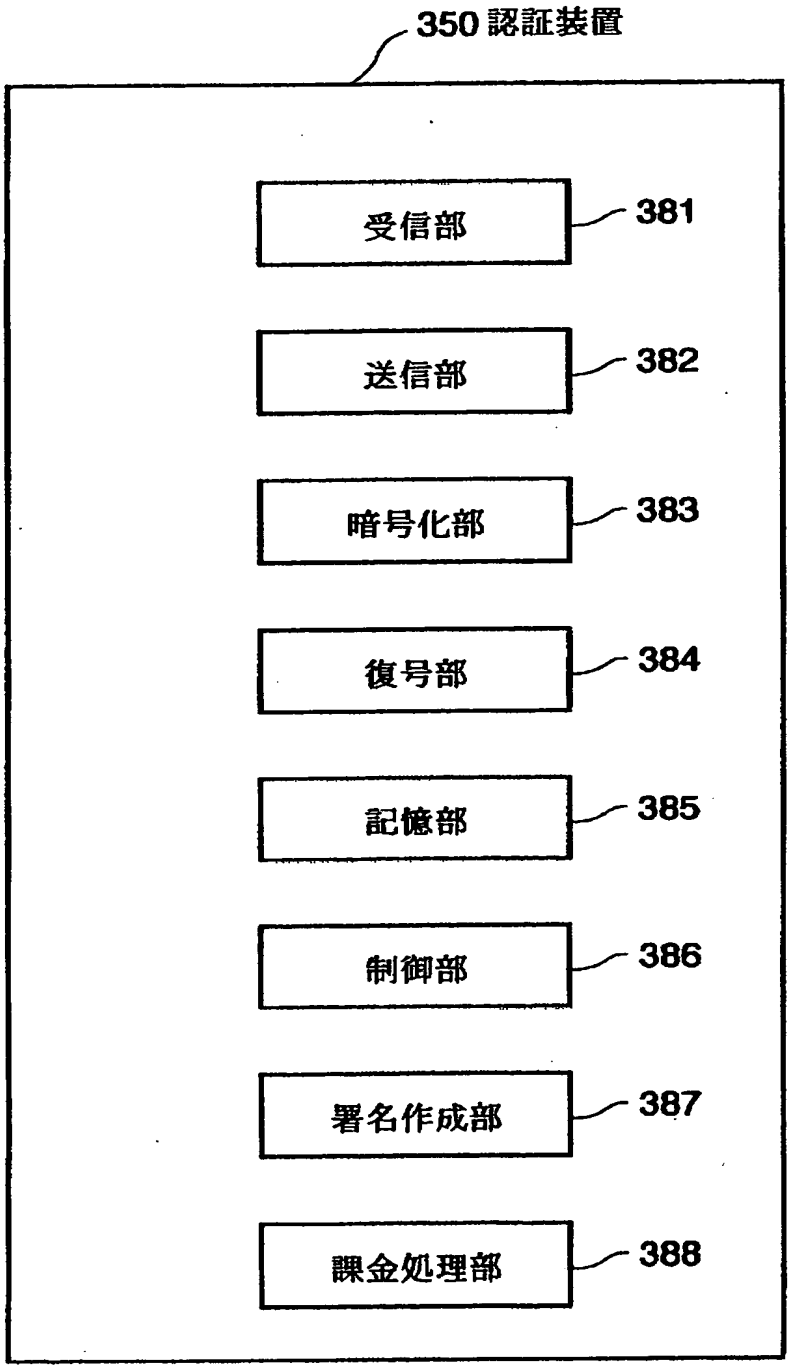
【図１２】


311 発注者端末装置
受信部
361
送信部
362
暗号化部
363
復号部
364
記憶部
365
制御部
366
署名検証部
367

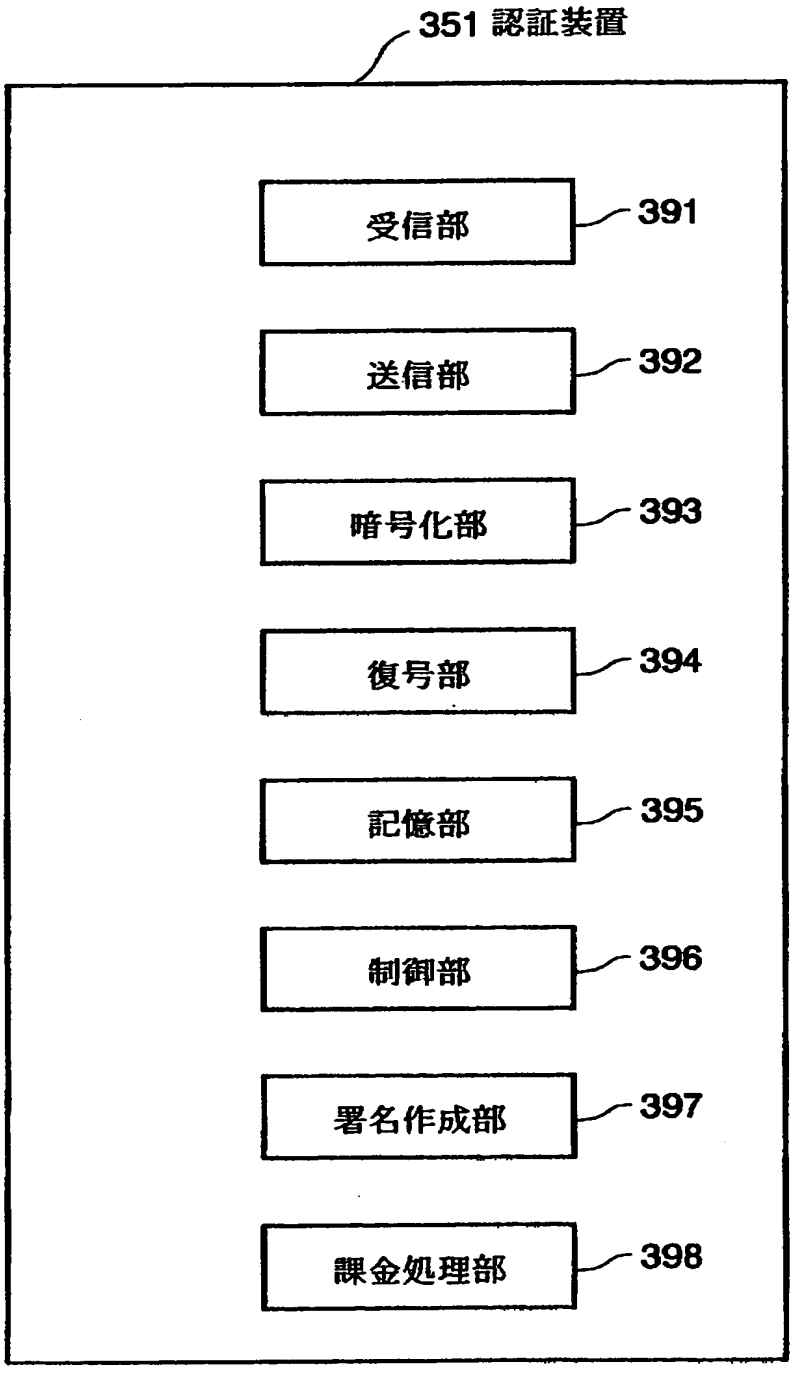
【図１３】



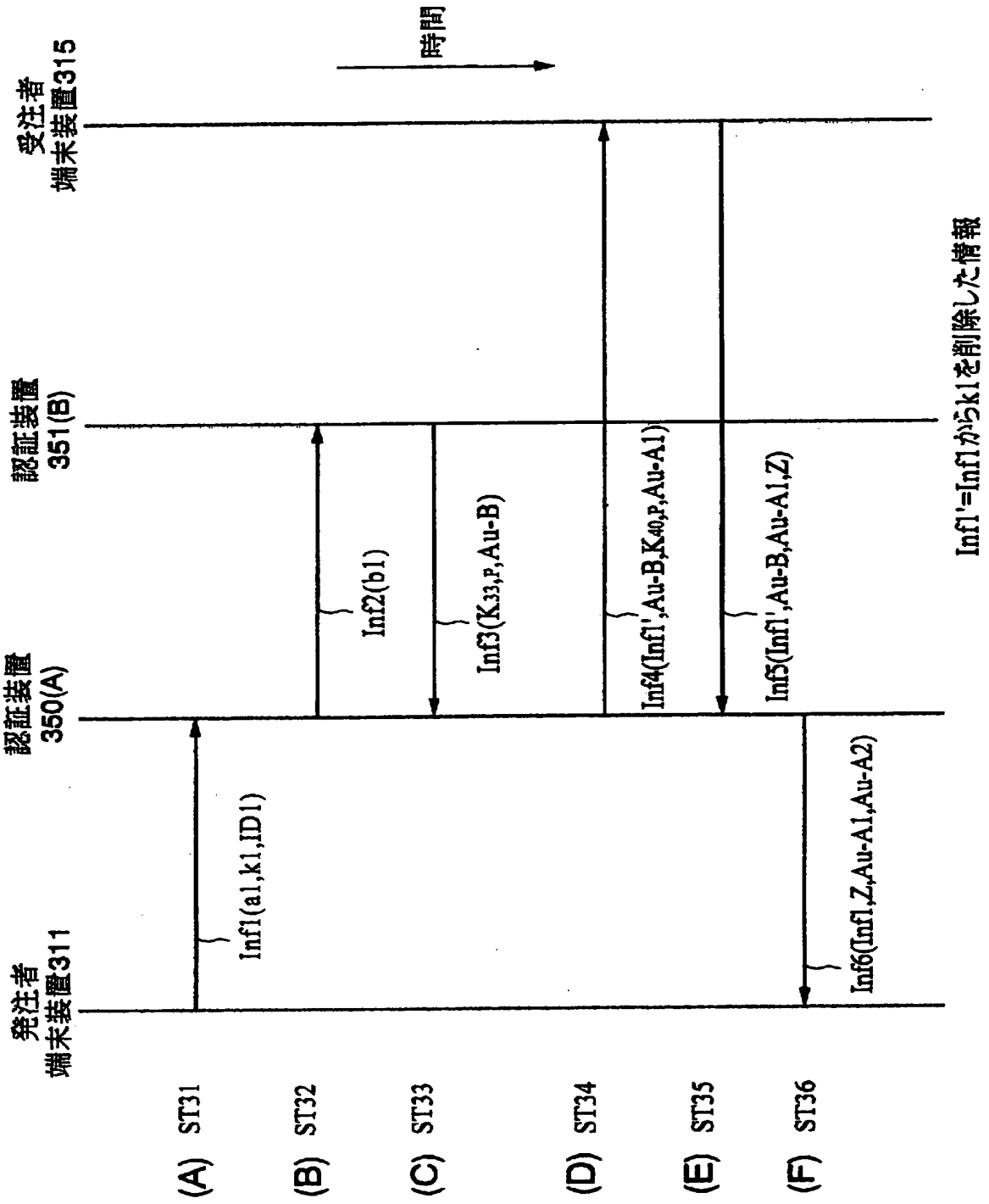
【図１４】


350 認証装置
受信部
381
送信部
382
暗号化部
383
復号部
384
記憶部
385
制御部
386
署名作成部
387
課金処理部
388

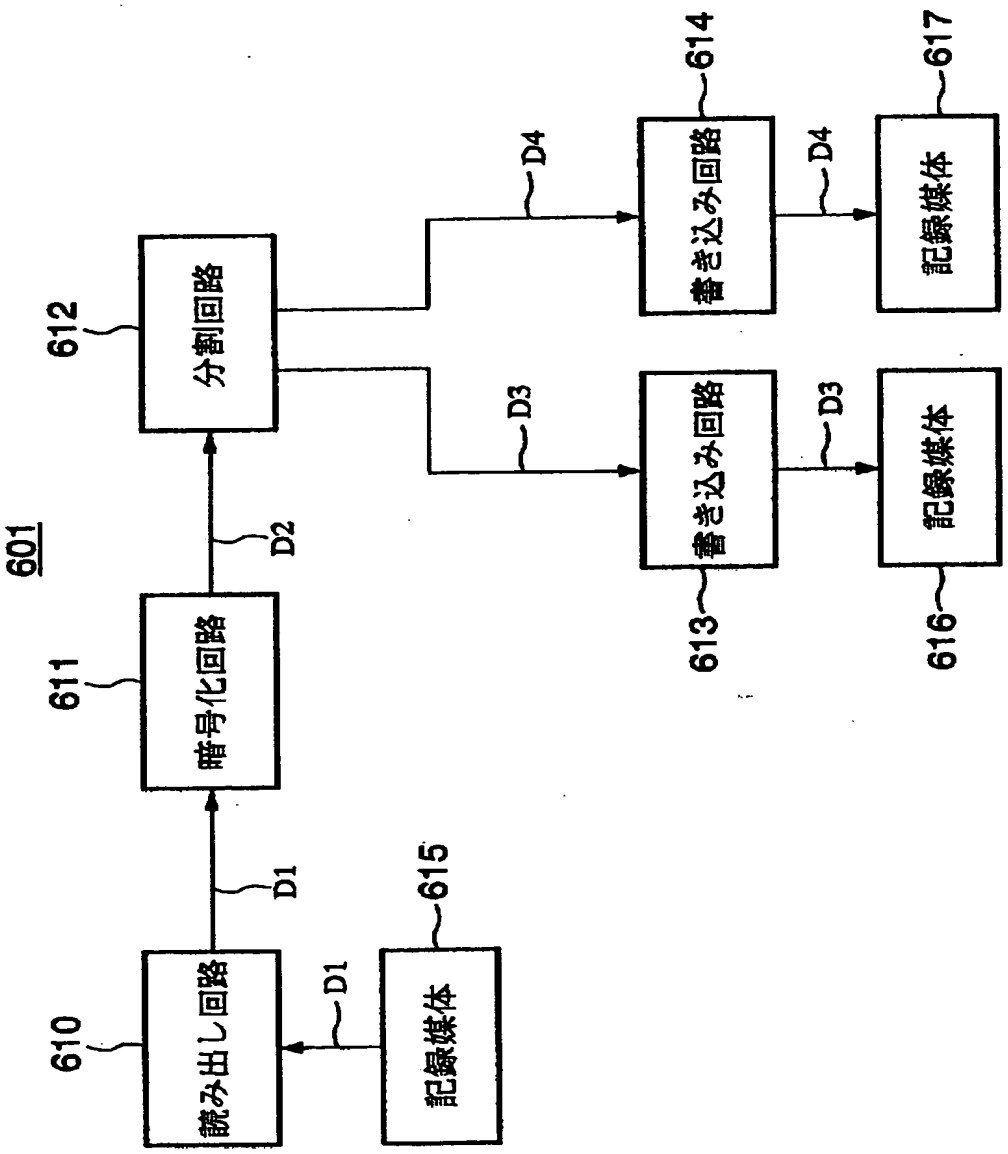
【図１５】


351 認証装置
受信部
391
送信部
392
暗号化部
393
復号部
394
記憶部
395
制御部
396
署名作成部
397
課金処理部
398

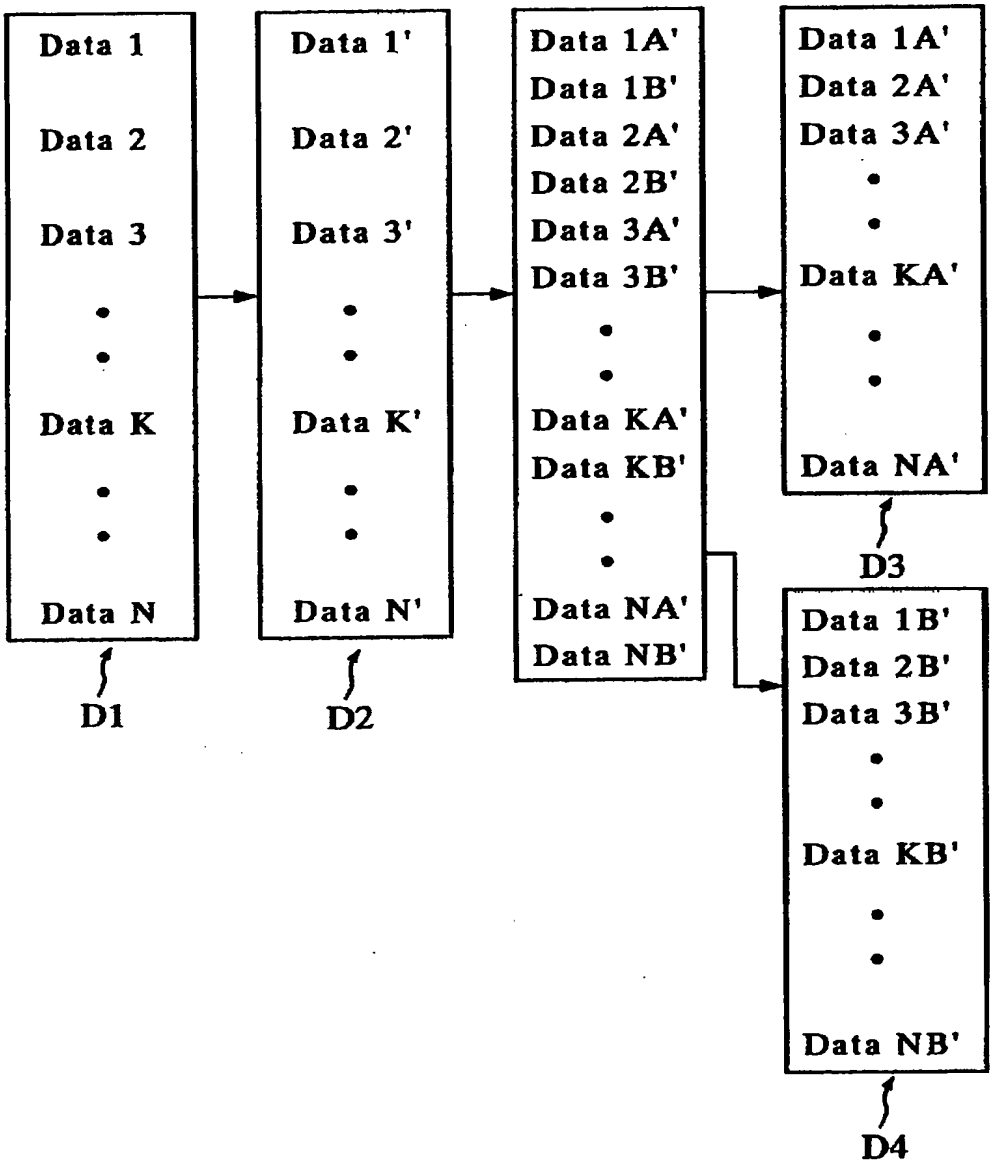
【図１６】


時間
受注者
端末装置315
認証装置
351(B)
認証装置
350(A)
発注者
端末装置311
Inf1(a1,k1,ID1)
Inf2(b1)
Inf3(K33,P,Au-B)
Inf4(Inf1',Au-B,K40,P,Au-A1)
Inf5(Inf1',Au-B,Au-A1,Z)
Inf6(Inf1,Z,Au-A1,Au-A2)
Inf1'=Inf1からk1を削除した情報
(A) ST31
(B) ST32
(C) ST33
(D) ST34
(E) ST35
(F) ST36

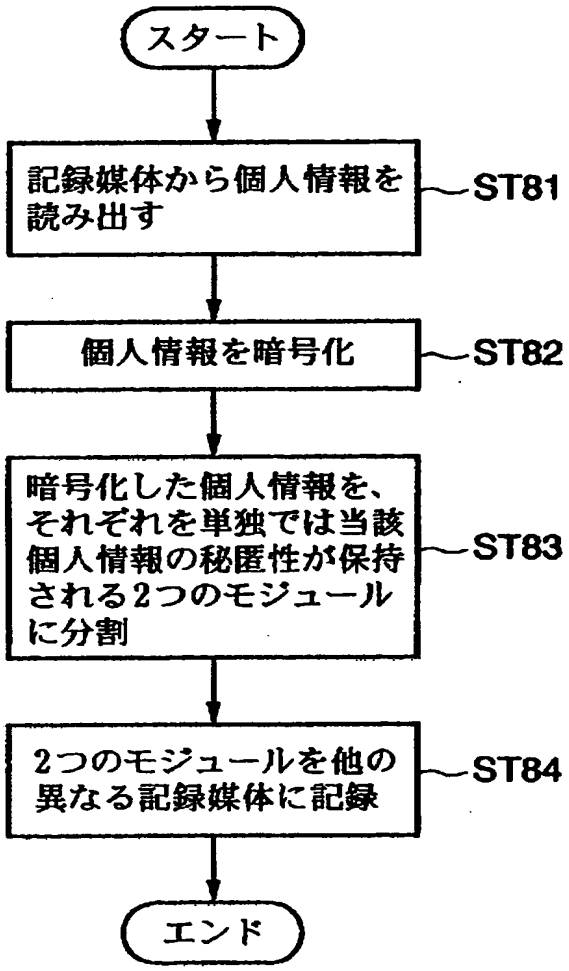
【図１７】


601
610
読み出し回路
615
記録媒体
D1
611
暗号化回路
D2
612
分割回路
D3
D4
613
書き込み回路
614
書き込み回路
616
記録媒体
617
記録媒体

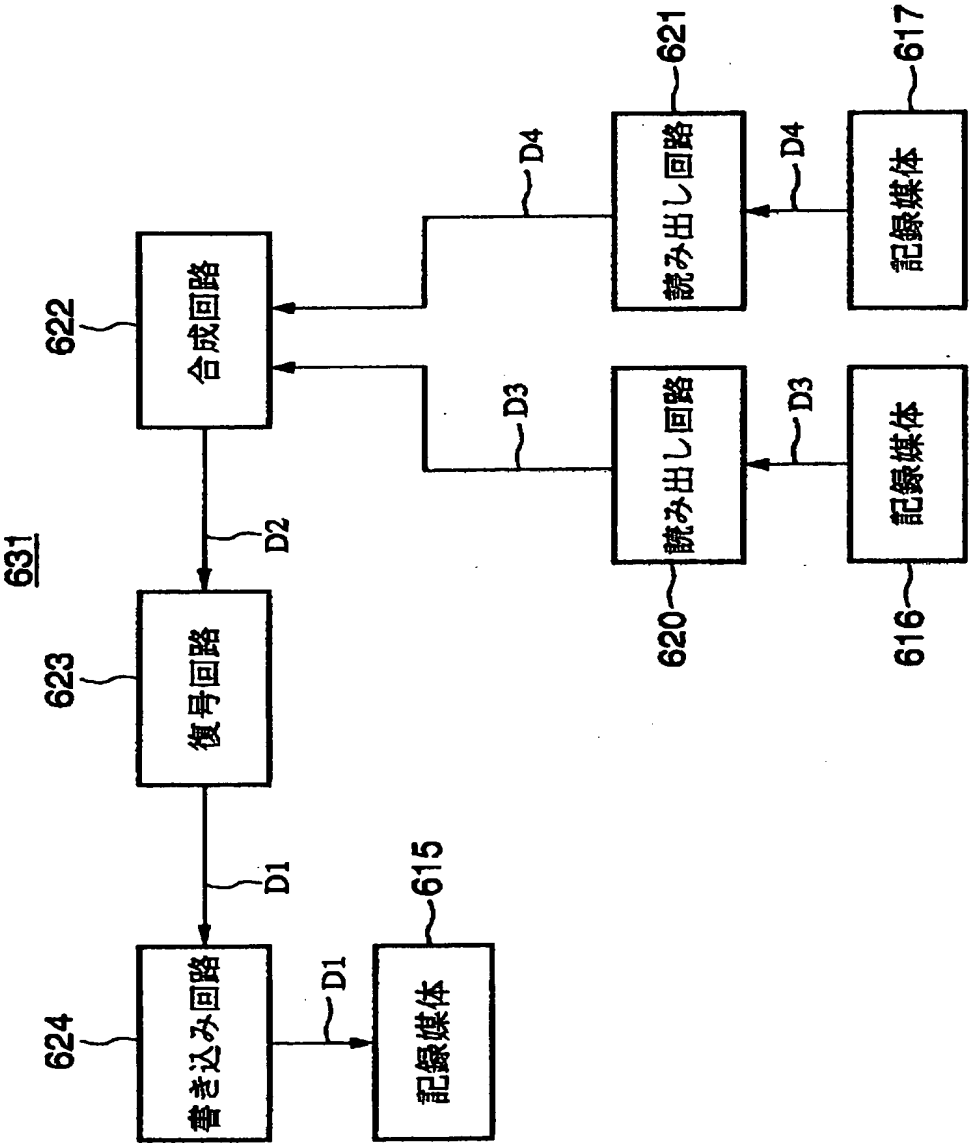
【図１８】


Data 1
Data 2
Data 3
Data K
Data N
D1
Data 1'
Data 2'
Data 3'
Data K'
Data N'
D2
Data 1A'
Data 1B'
Data 2A'
Data 2B'
Data 3A'
Data 3B'
Data KA'
Data KB'
Data NA'
Data NB'
Data 1A'
Data 2A'
Data 3A'
Data KA'
Data NA'
D3
Data 1B'
Data 2B'
Data 3B'
Data KB'
Data NB'
D4

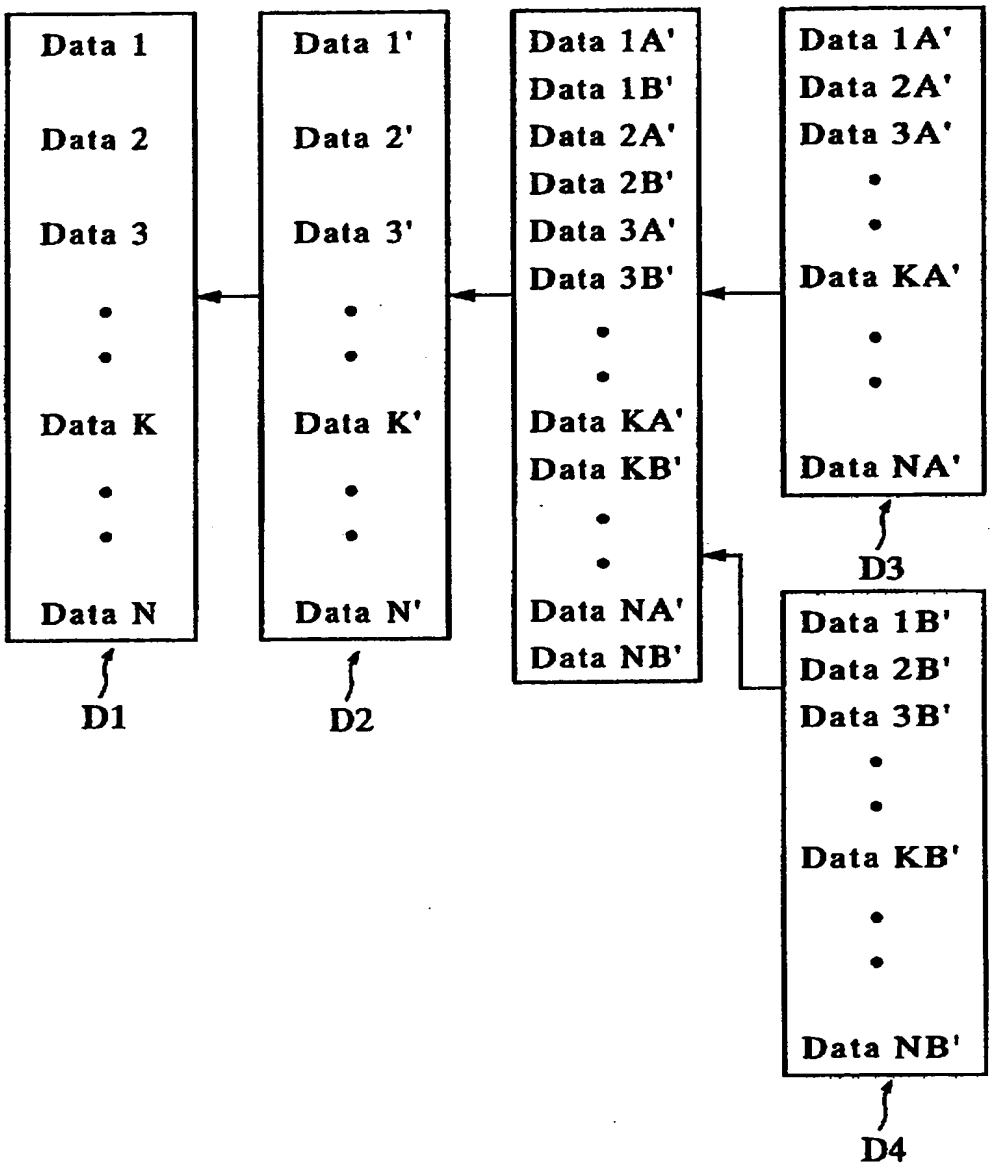
【図１９】


スタート
記録媒体から個人情報を読み出す
ST81
個人情報を暗号化
ST82
暗号化した個人情報を、それぞれを単独では当該個人情報の秘匿性が保持される2つのモジュールに分割
ST83
2つのモジュールを他の異なる記録媒体に記録
ST84
エンド

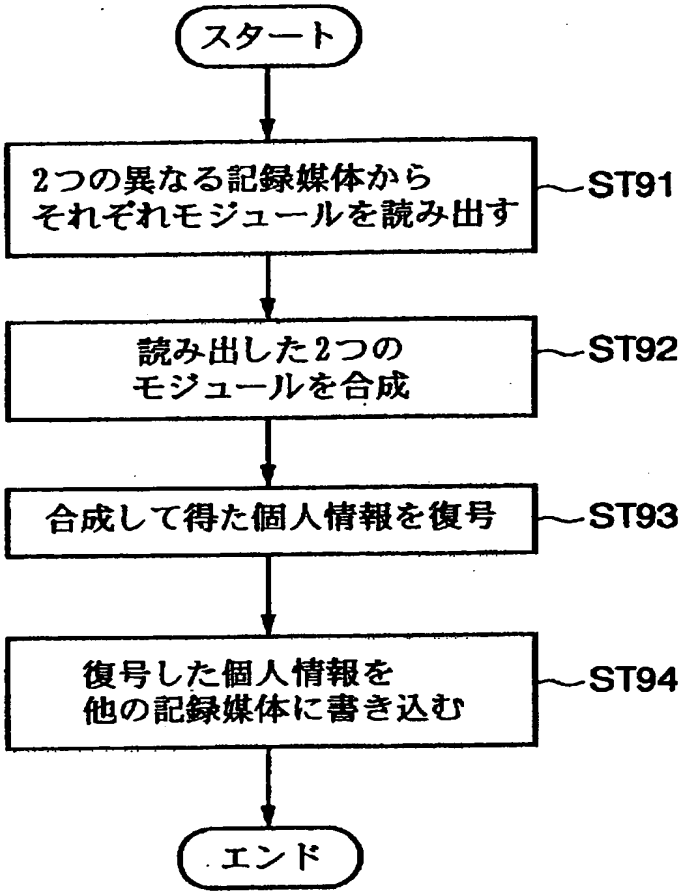
【図２０】


631
622
合成回路
623
復号回路
624
書き込み回路
615
記録媒体
620
読み出し回路
616
記録媒体
621
読み出し回路
617
記録媒体
D1
D2
D3
D4
D1
D3
D4

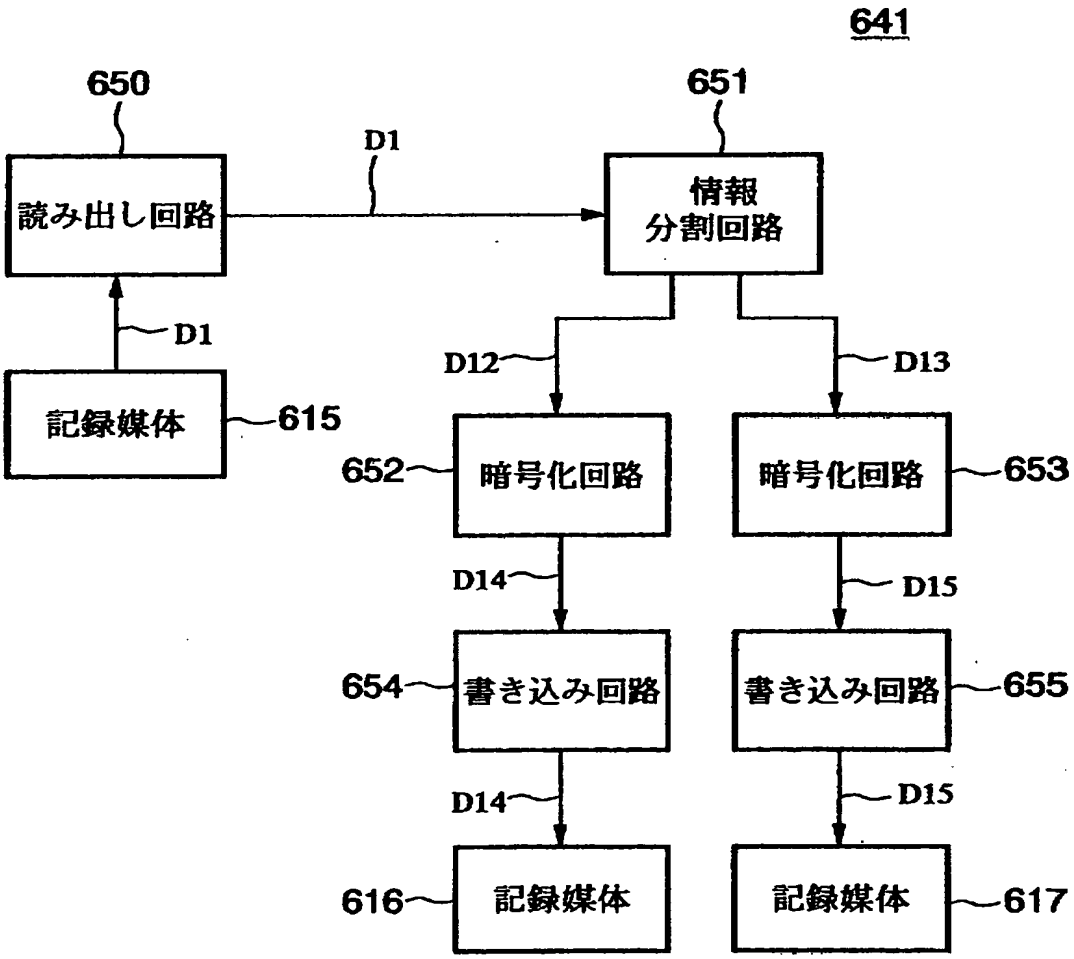
【図２１】


Data 1
Data 2
Data 3
Data K
Data N
D1
Data 1'
Data 2'
Data 3'
Data K'
Data N'
D2
Data 1A'
Data 1B'
Data 2A'
Data 2B'
Data 3A'
Data 3B'
Data KA'
Data KB'
Data NA'
Data NB'
Data 1A'
Data 2A'
Data 3A'
Data KA'
Data NA'
D3
Data 1B'
Data 2B'
Data 3B'
Data KB'
Data NB'
D4

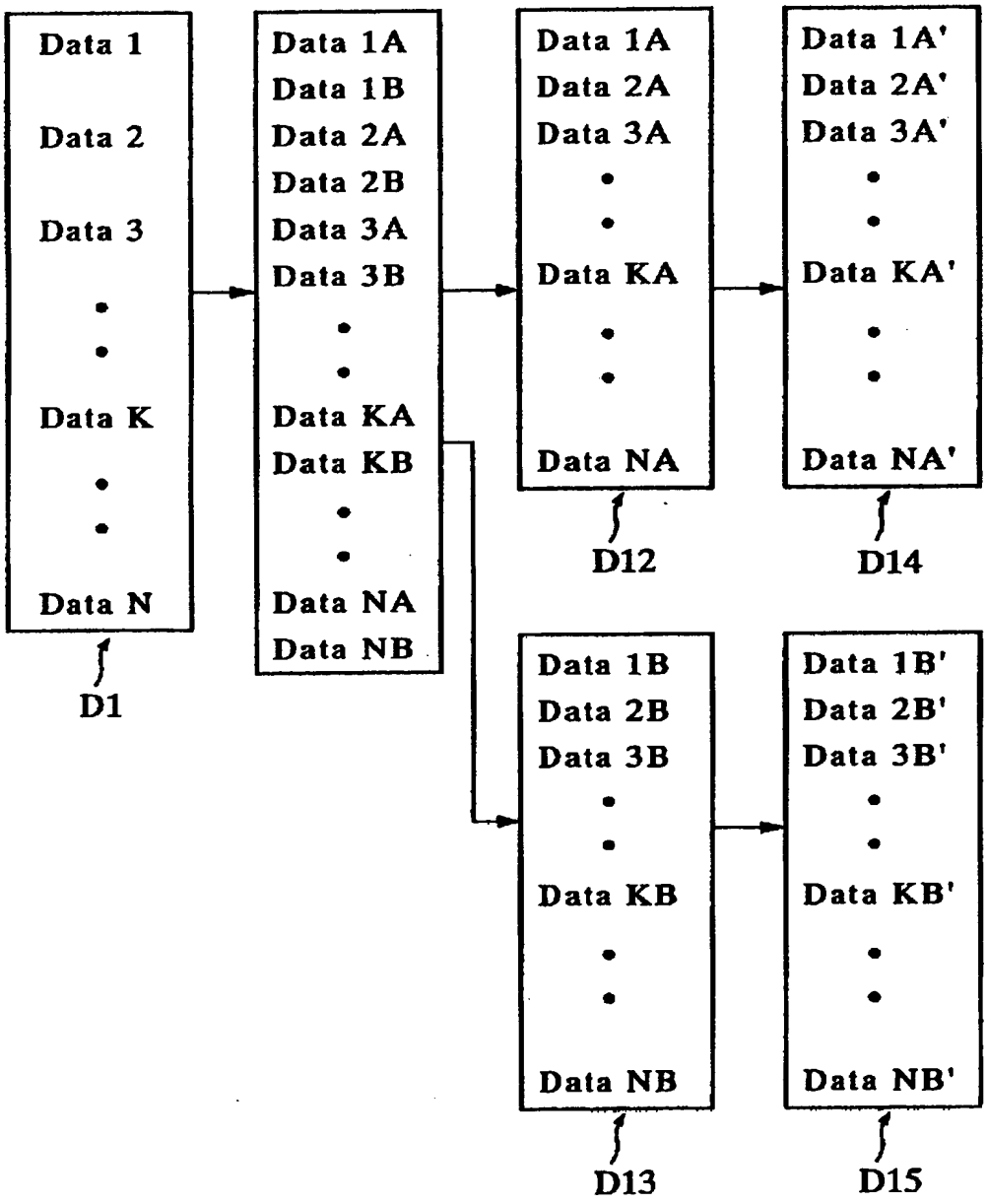
【図２２】


スタート
2つの異なる記録媒体から
それぞれモジュールを読み出す
ST91
読み出した2つの
モジュールを合成
ST92
合成して得た個人情報を復号
ST93
復号した個人情報を
他の記録媒体に書き込む
ST94
エンド

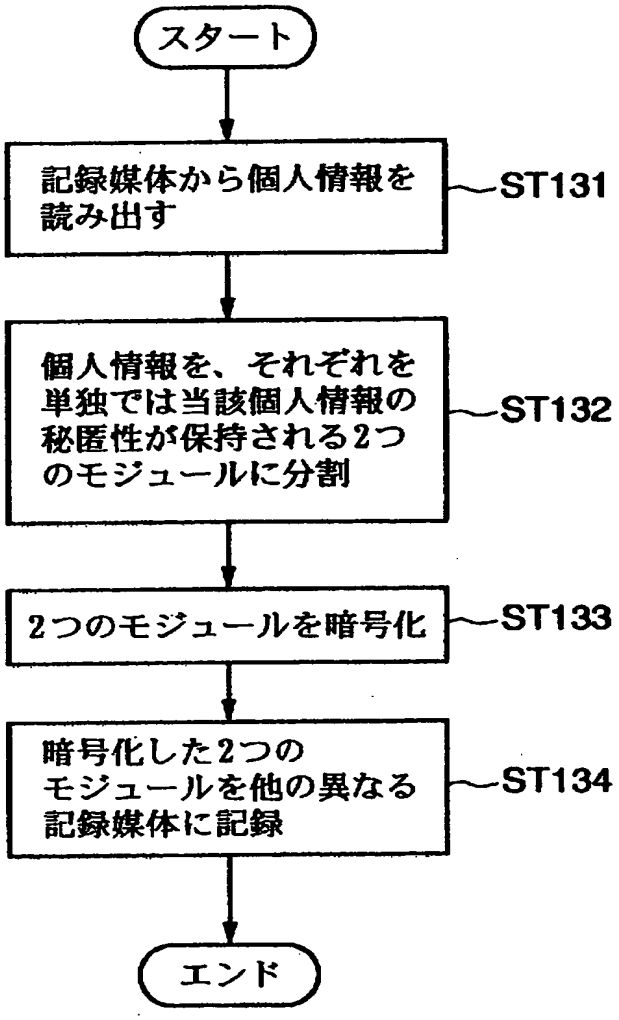
【図２３】


641
650
651
D1
読み出し回路
情報
分割回路
D1
D12
D13
記録媒体
615
652
暗号化回路
暗号化回路
653
D14
D15
654
書き込み回路
書き込み回路
655
D14
D15
616
記録媒体
記録媒体
617

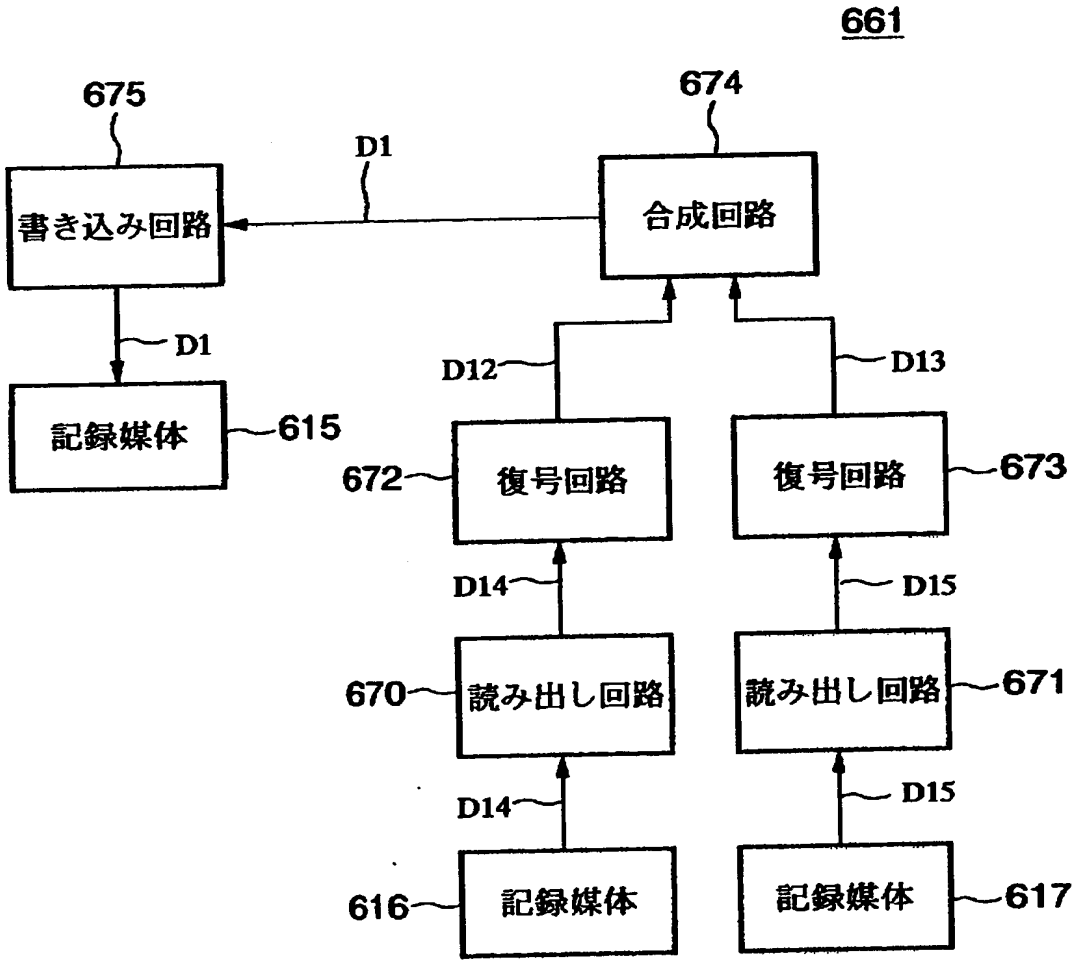
【図２４】


Data 1
Data 2
Data 3
Data K
Data N
D1
Data 1A
Data 1B
Data 2A
Data 2B
Data 3A
Data 3B
Data KA
Data KB
Data NA
Data NB
Data 1A
Data 2A
Data 3A
Data KA
Data NA
D12
Data 1A'
Data 2A'
Data 3A'
Data KA'
Data NA'
D14
Data 1B
Data 2B
Data 3B
Data KB
Data NB
D13
Data 1B'
Data 2B'
Data 3B'
Data KB'
Data NB'
D15

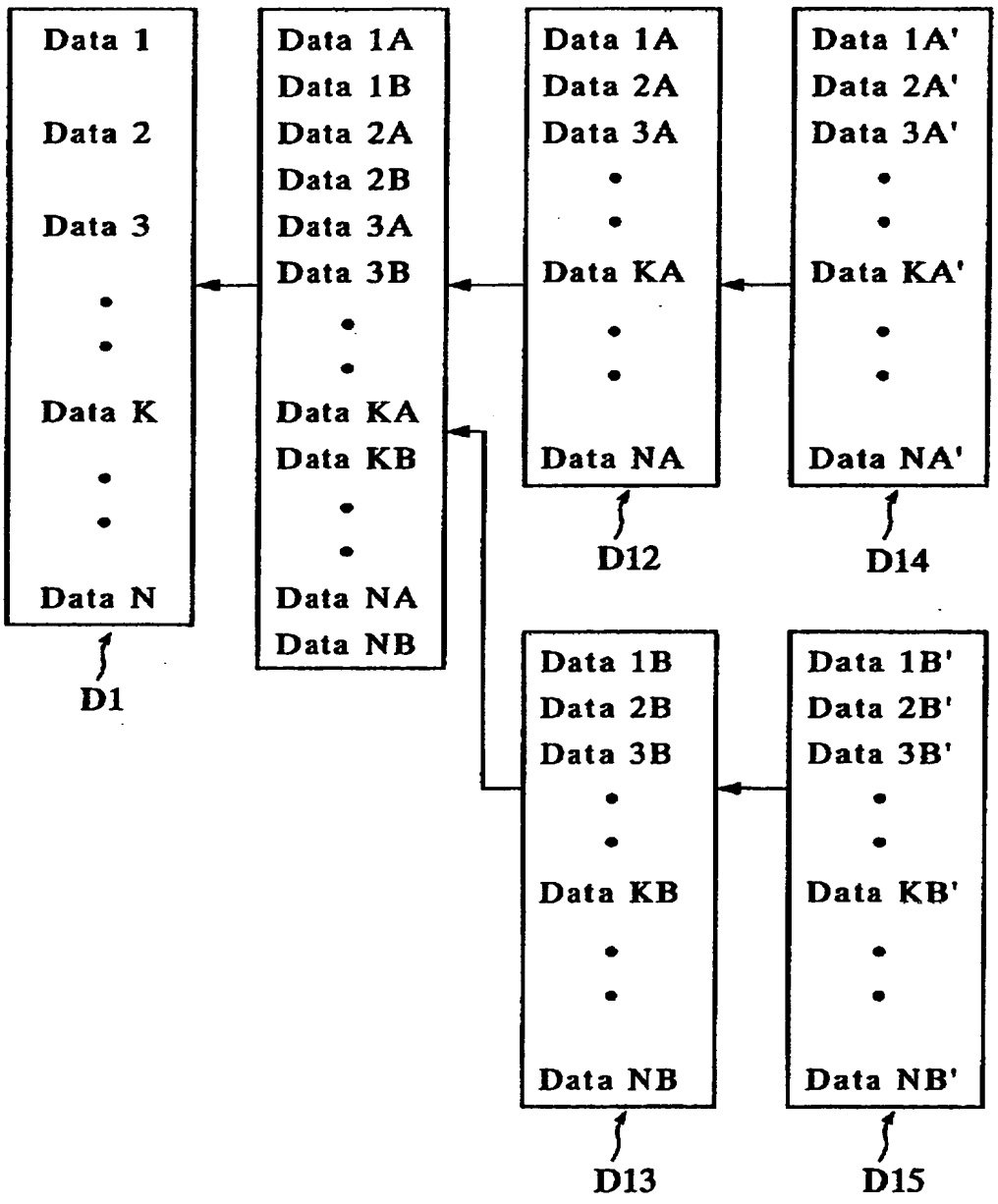
【図２５】


スタート
記録媒体から個人情報を読み出す
ST131
個人情報を、それぞれを単独では当該個人情報の秘匿性が保持される2つのモジュールに分割
ST132
2つのモジュールを暗号化
ST133
暗号化した2つのモジュールを他の異なる記録媒体に記録
ST134
エンド

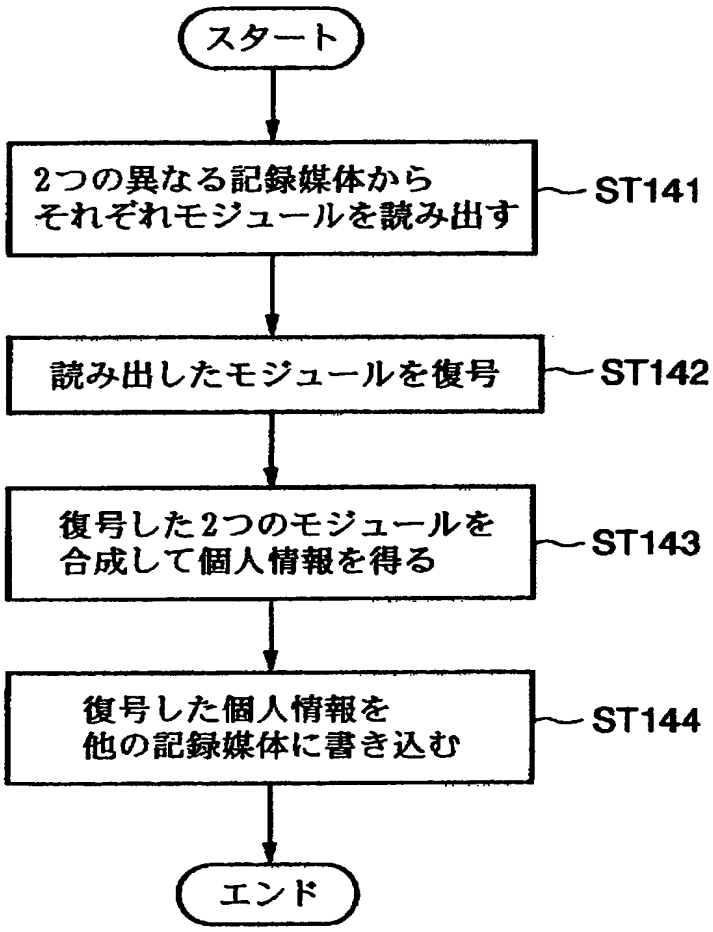
【図２６】


661
675
674
D1
書き込み回路
合成回路
D1
D12
D13
記録媒体
615
672
復号回路
復号回路
673
D14
D15
670
読み出し回路
読み出し回路
671
D14
D15
616
記録媒体
記録媒体
617

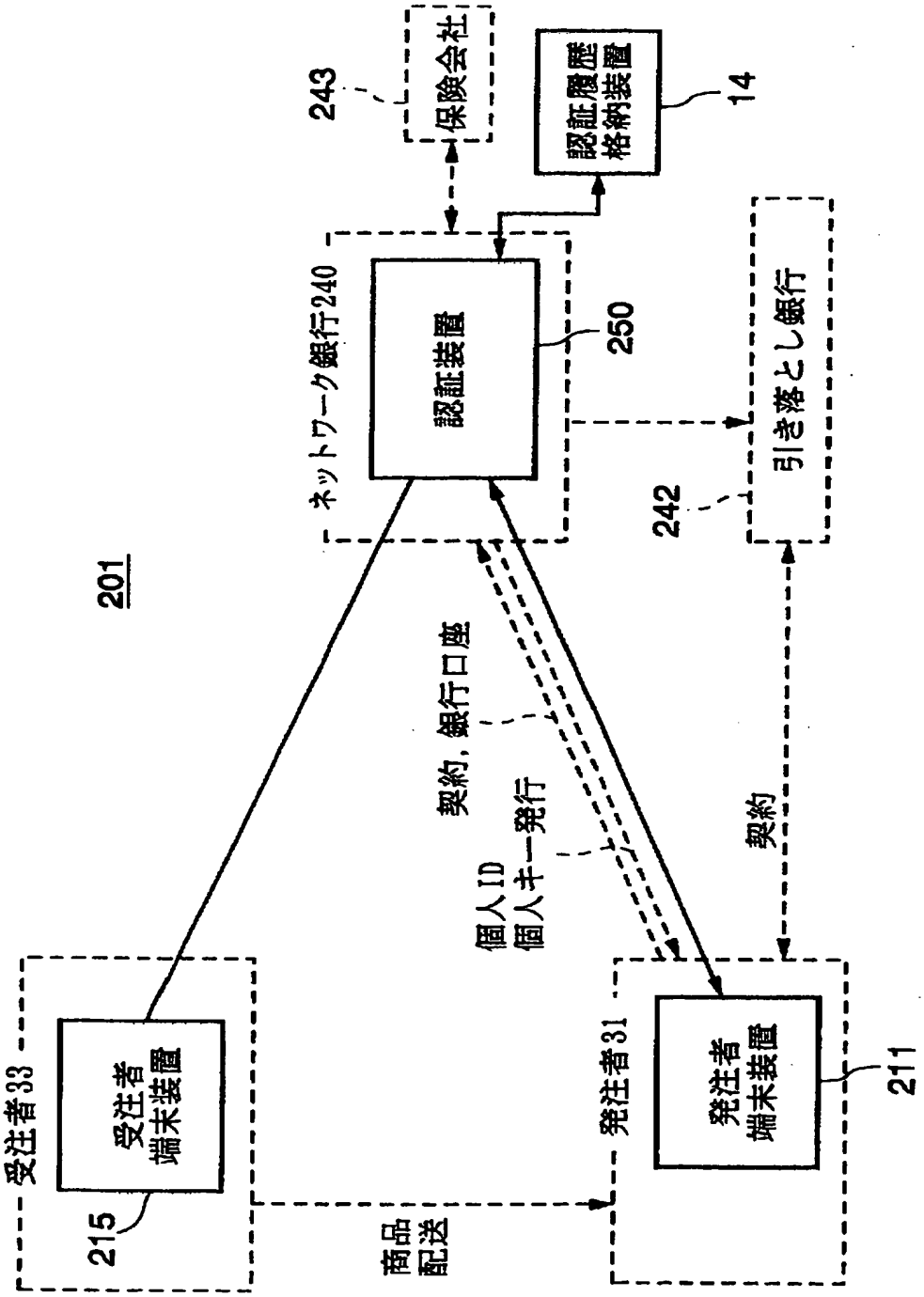
【図２７】


Data 1
Data 2
Data 3
Data K
Data N
D1
Data 1A
Data 1B
Data 2A
Data 2B
Data 3A
Data 3B
Data KA
Data KB
Data NA
Data NB
Data 1A
Data 2A
Data 3A
Data KA
Data NA
D12
Data 1A'
Data 2A'
Data 3A'
Data KA'
Data NA'
D14
Data 1B
Data 2B
Data 3B
Data KB
Data NB
D13
Data 1B'
Data 2B'
Data 3B'
Data KB'
Data NB'
D15

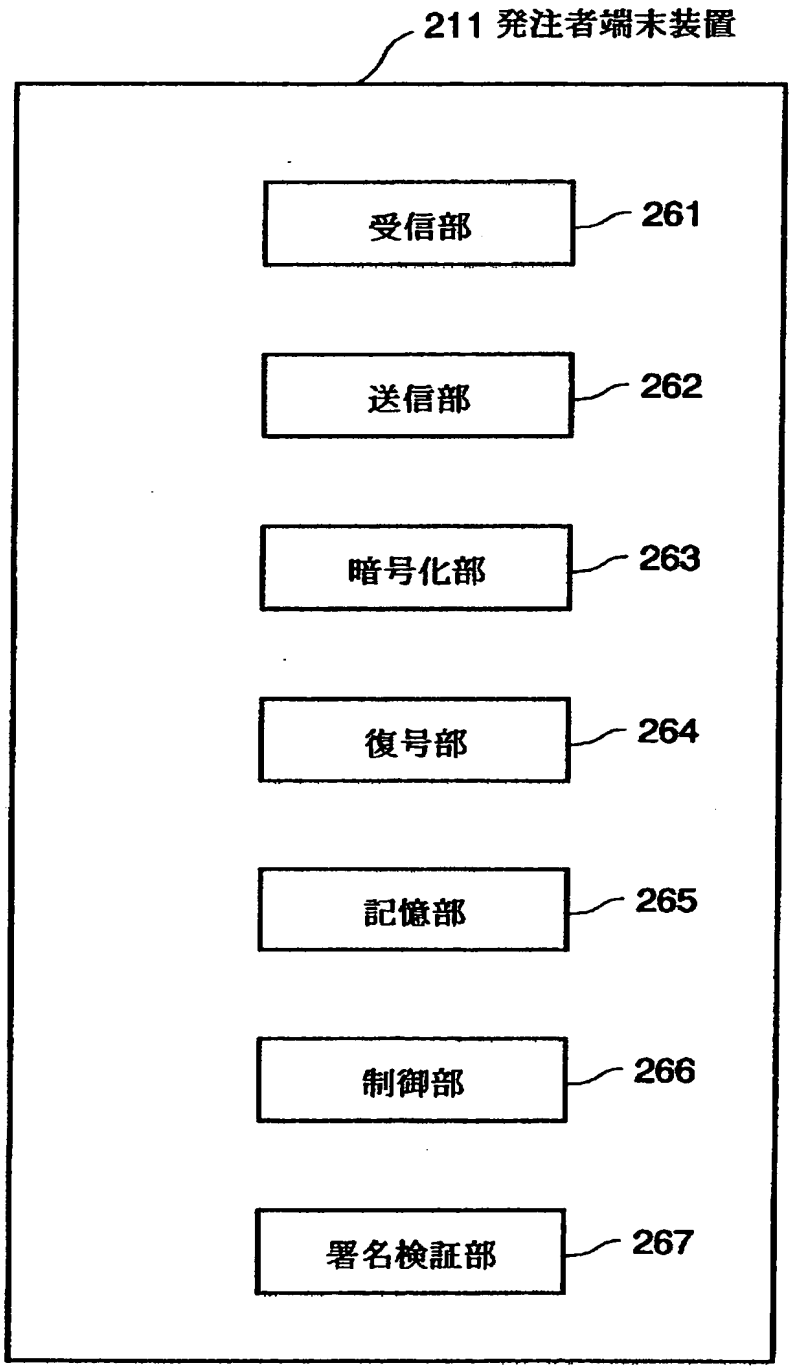
【図２８】


スタート
2つの異なる記録媒体から
それぞれモジュールを読み出す
ST141
読み出したモジュールを復号
ST142
復号した2つのモジュールを
合成して個人情報を得る
ST143
復号した個人情報を
他の記録媒体に書き込む
ST144
エンド

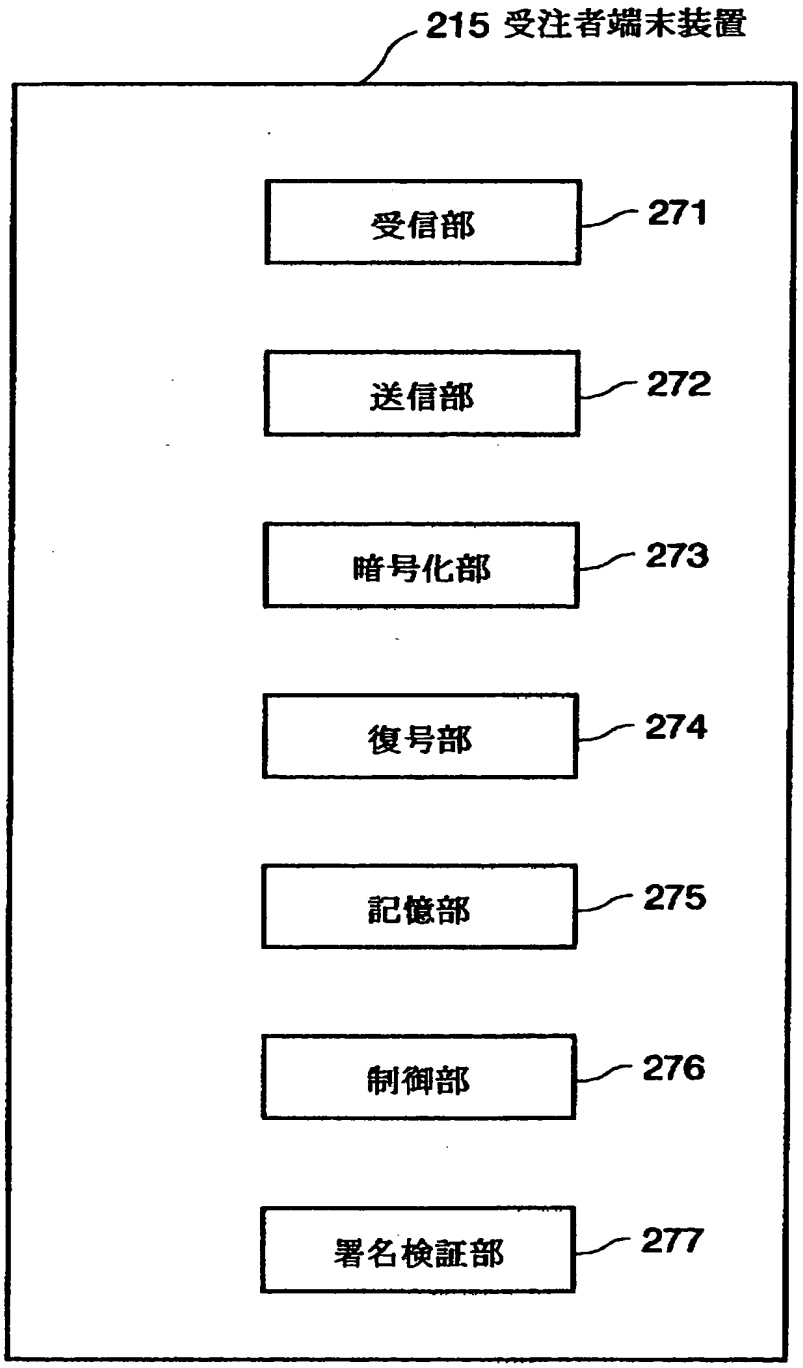
【図２９】


201
ネットワーク銀行240
認証装置
250
保険会社
243
認証履歴
格納装置
14
引き落とし銀行
242
契約，銀行口座
個人ID
個人キー発行
契約
受注者33
受注者
端末装置
215
商品
配送
発注者31
発注者
端末装置
211

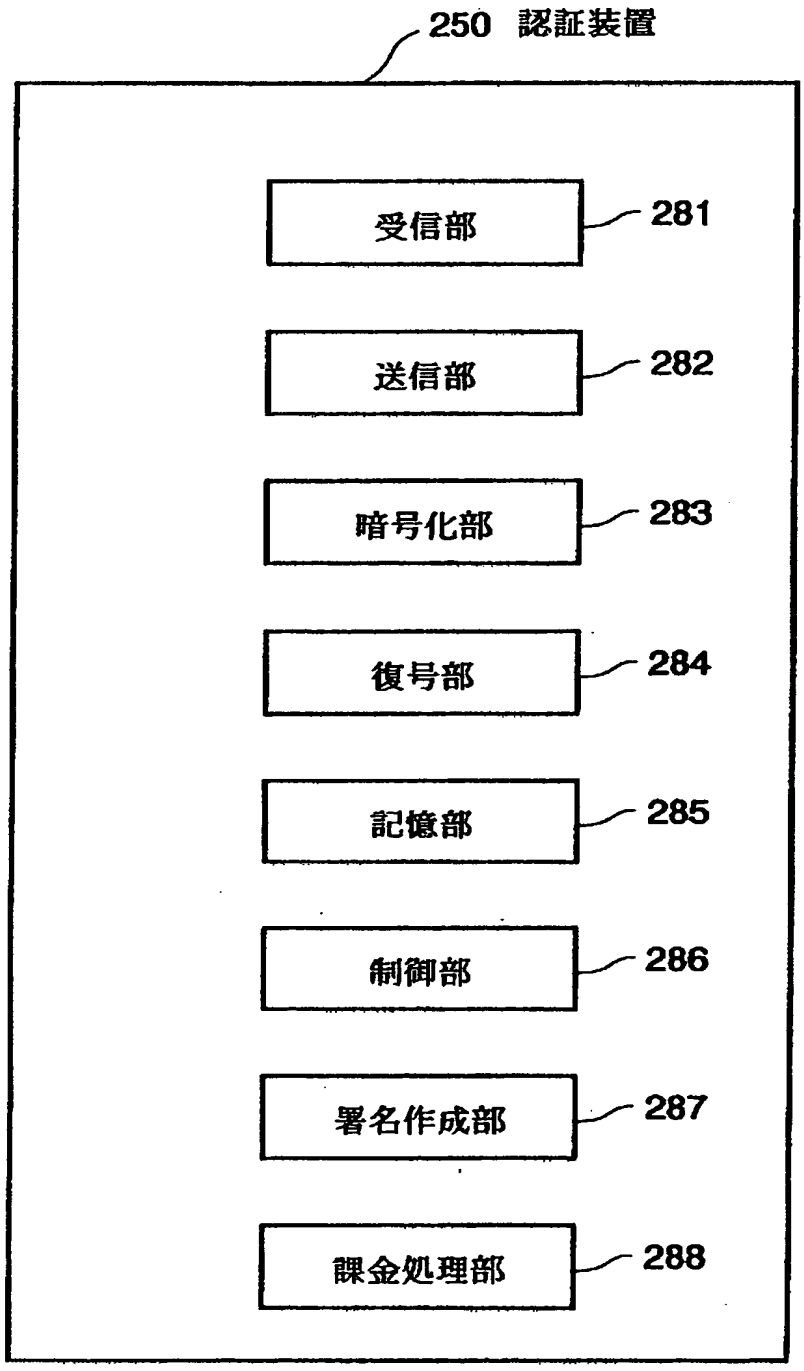
【図３０】


211 発注者端末装置
受信部
261
送信部
262
暗号化部
263
復号部
264
記憶部
265
制御部
266
署名検証部
267

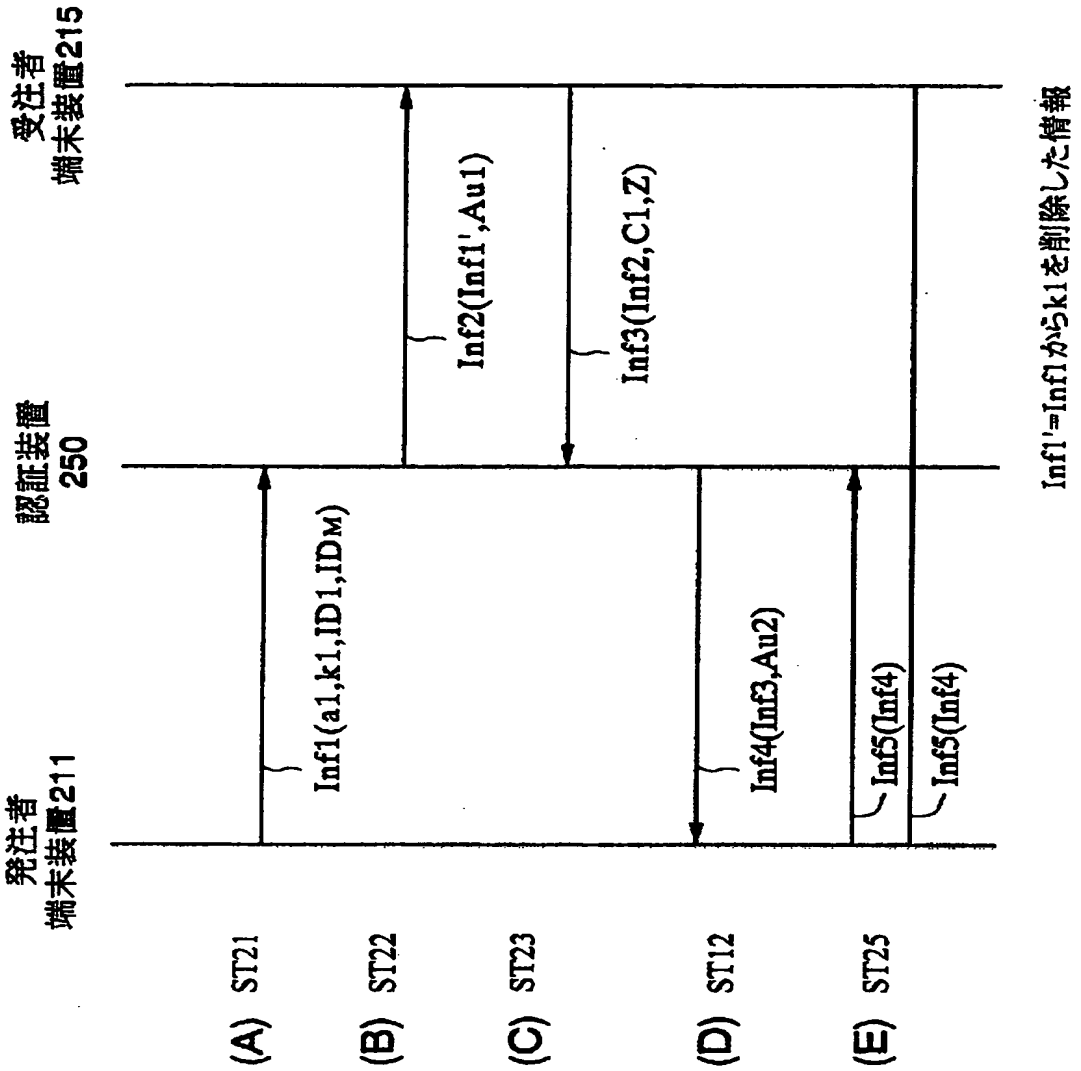
【図３１】


215 受注者端末装置
受信部
271
送信部
272
暗号化部
273
復号部
274
記憶部
275
制御部
276
署名検証部
277

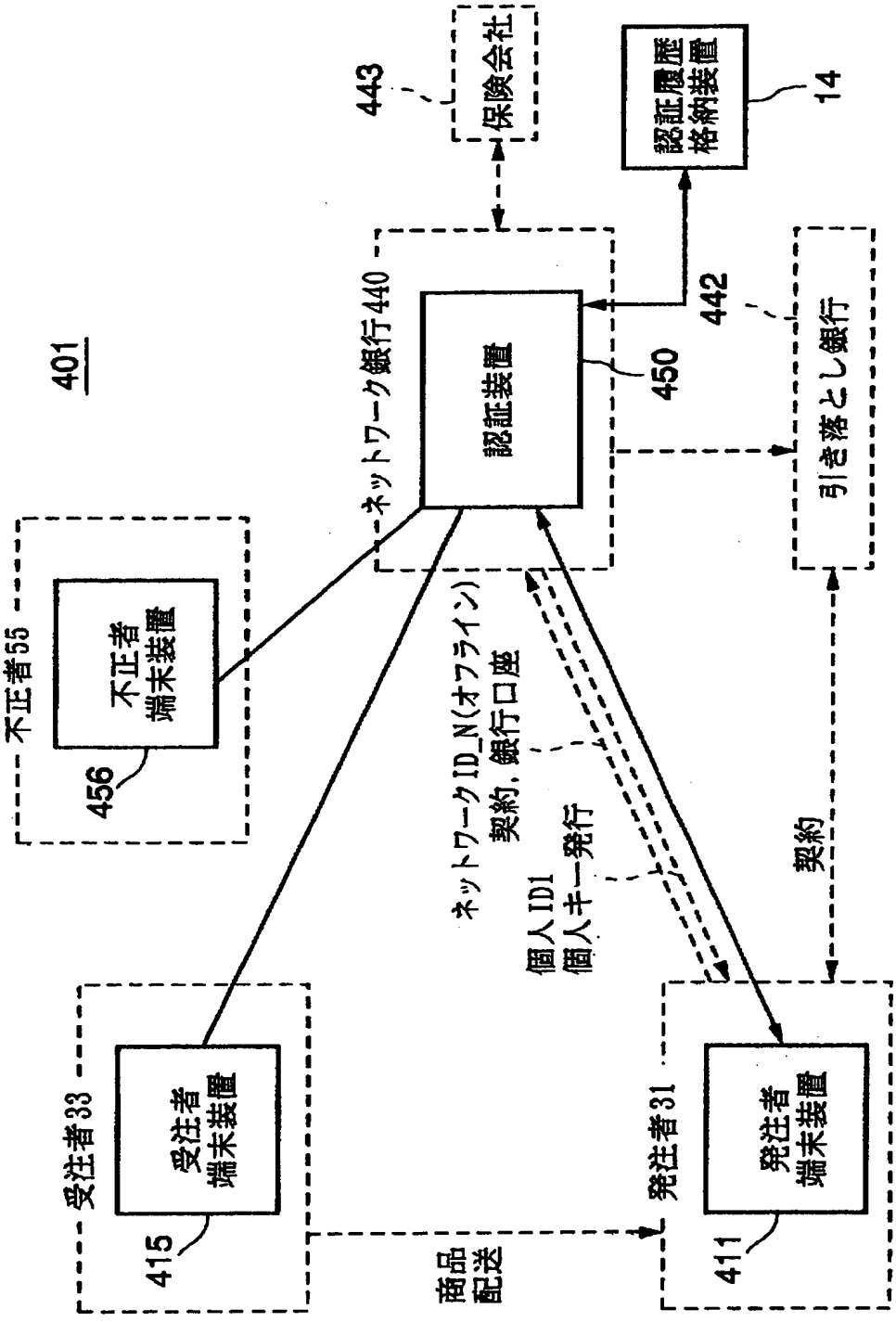
【図３２】


250 認証装置
受信部
281
送信部
282
暗号化部
283
復号部
284
記憶部
285
制御部
286
署名作成部
287
課金処理部
288

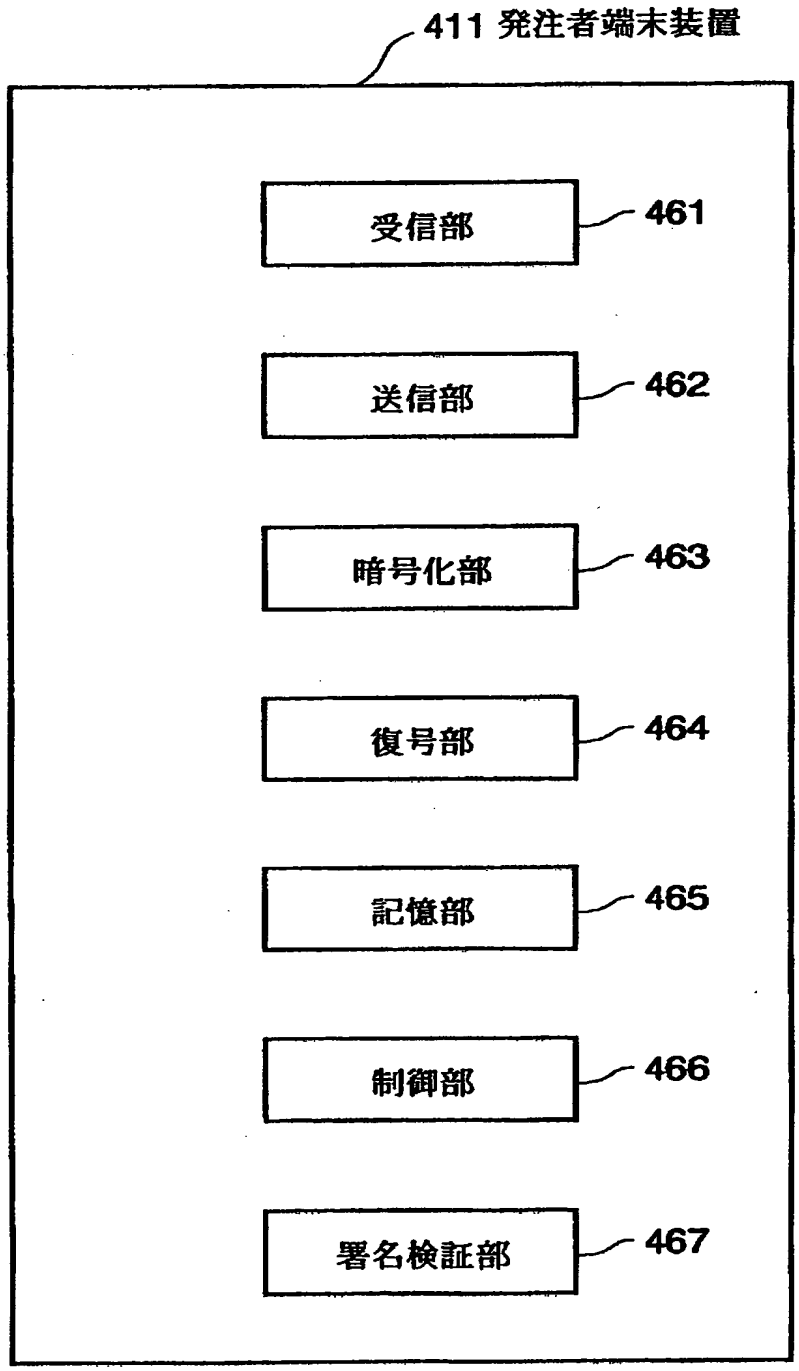
【図３３】


発注者
端末装置211
認証装置
250
受注者
端末装置215
Inf1(a1,k1,ID1,IDM)
Inf2(Inf1',Au1)
Inf3(Inf2,C1,Z)
Inf4(Inf3,Au2)
Inf5(Inf4)
Inf5(Inf4)
Inf1'=Inf1からk1を削除した情報
(A) ST21
(B) ST22
(C) ST23
(D) ST12
(E) ST25

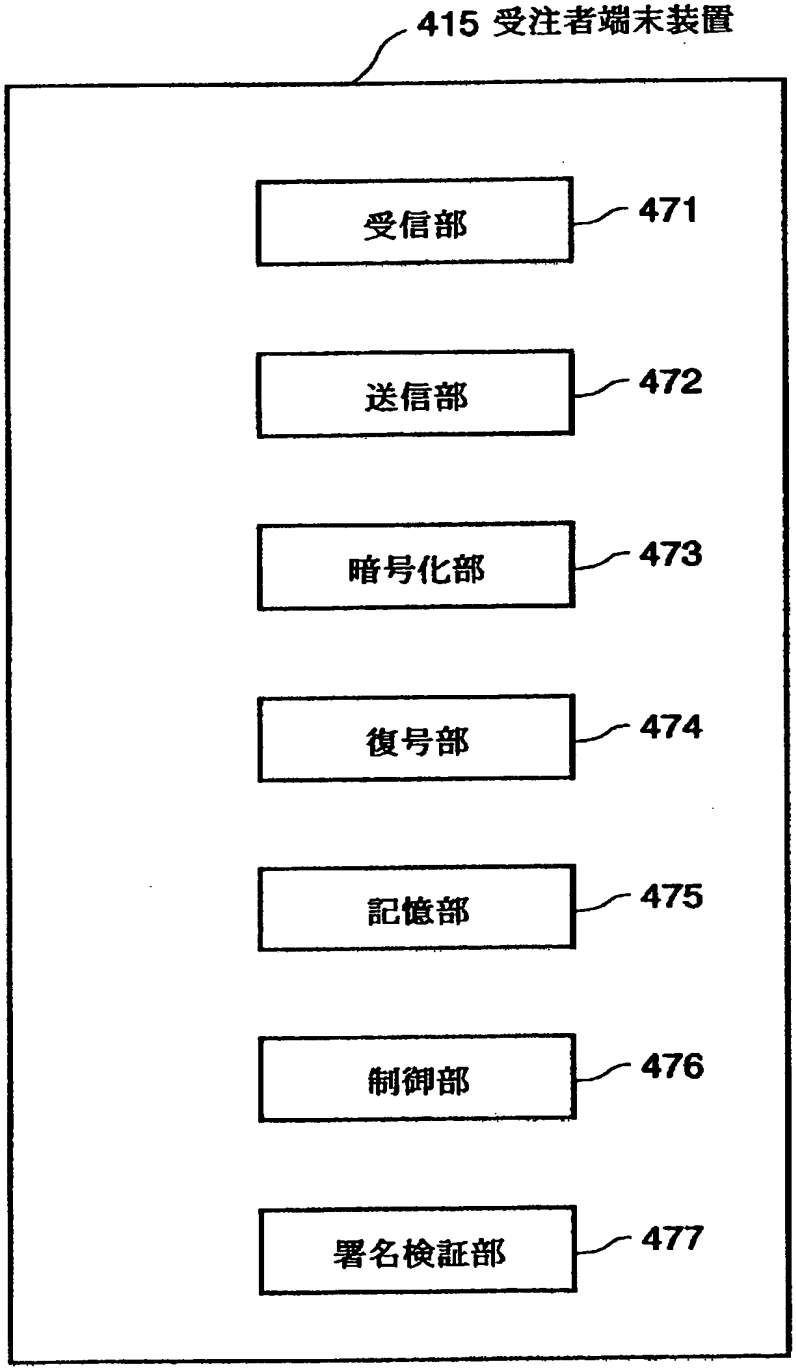
【図３４】


401
443
保険会社
認証履歴
格納装置
14
442
450
ネットワーク銀行440
認証装置
引き落とし銀行
不正者55
不正者
端末装置
456
ネットワークID_N(オフライン)
契約，銀行口座
個人ID1
個人キー発行
契約
受注者33
受注者
端末装置
415
商品
配送
発注者31
発注者
端末装置
411

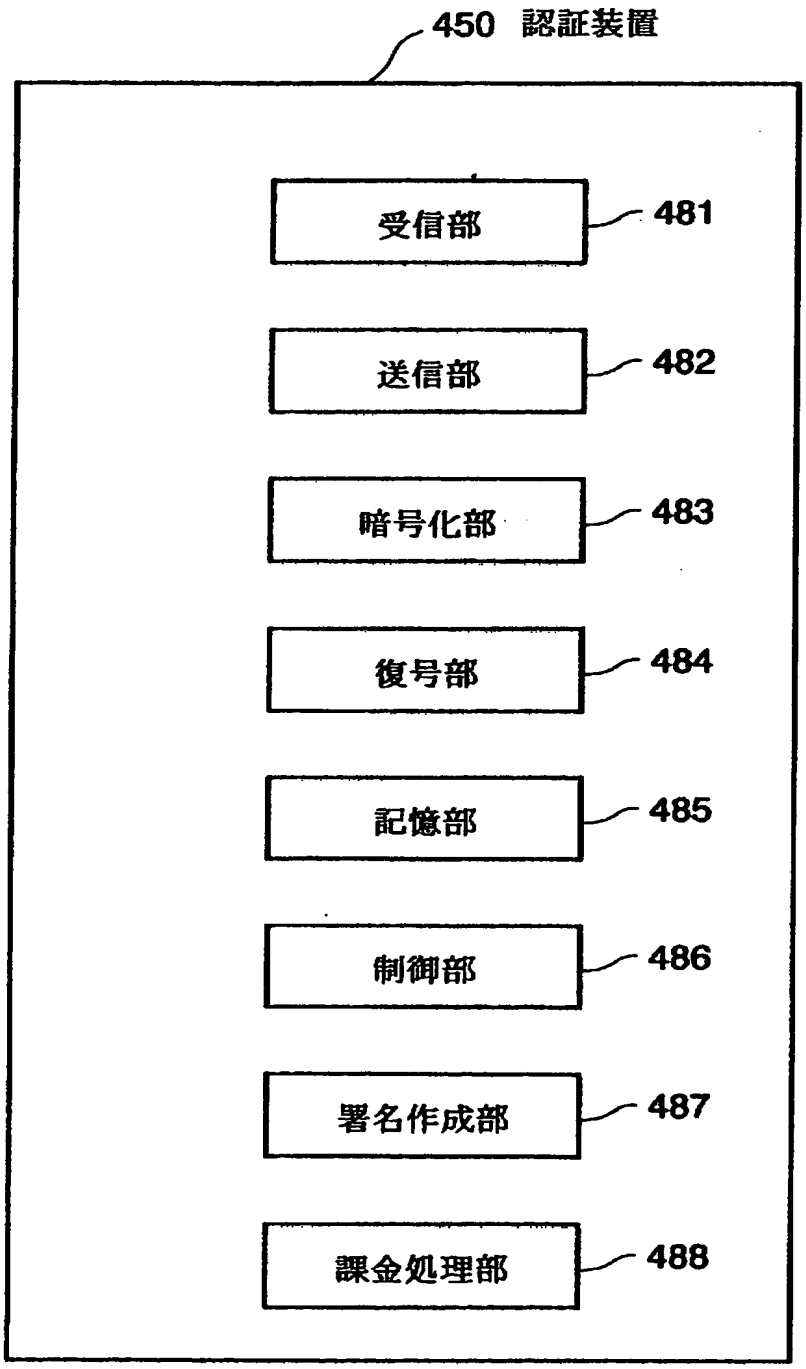
【図３５】


411 発注者端末装置
受信部
461
送信部
462
暗号化部
463
復号部
464
記憶部
465
制御部
466
署名検証部
467

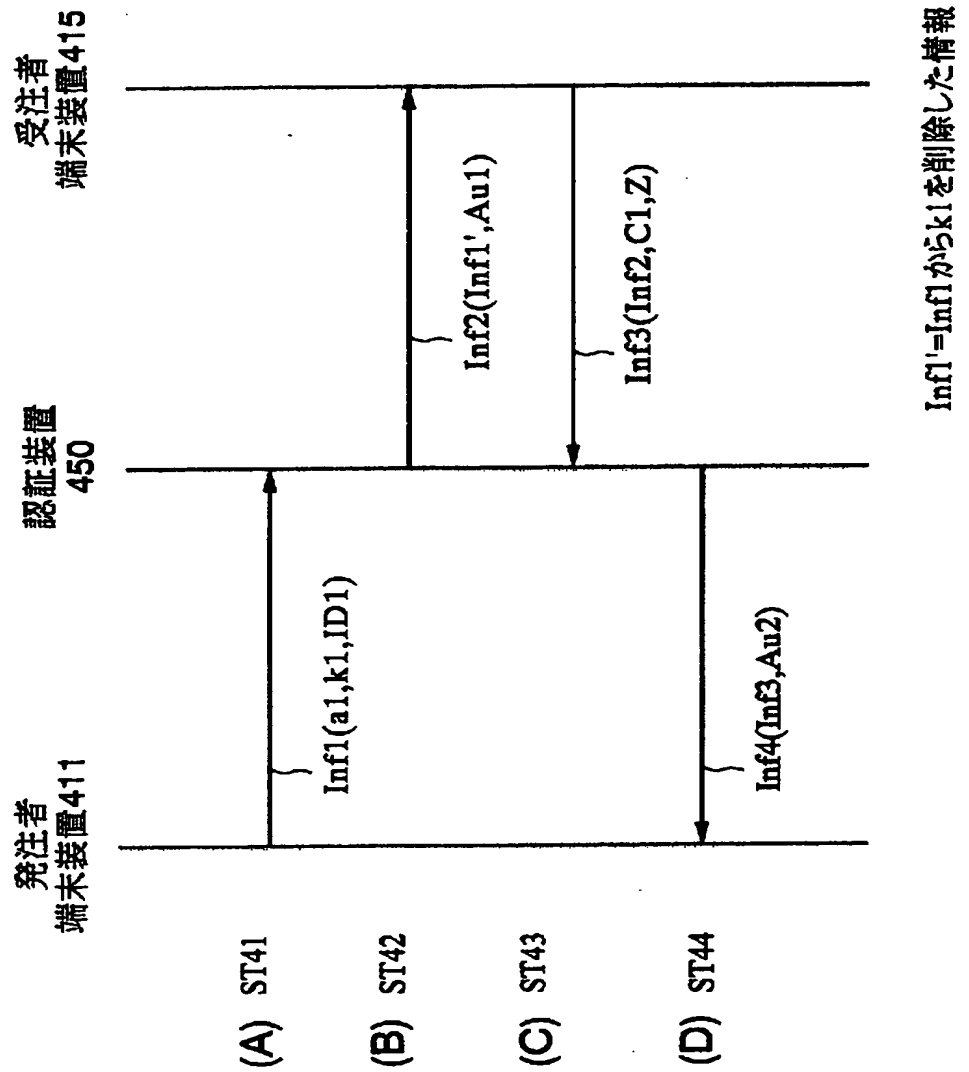
【図３６】


415 受注者端末装置
受信部
471
送信部
472
暗号化部
473
復号部
474
記憶部
475
制御部
476
署名検証部
477

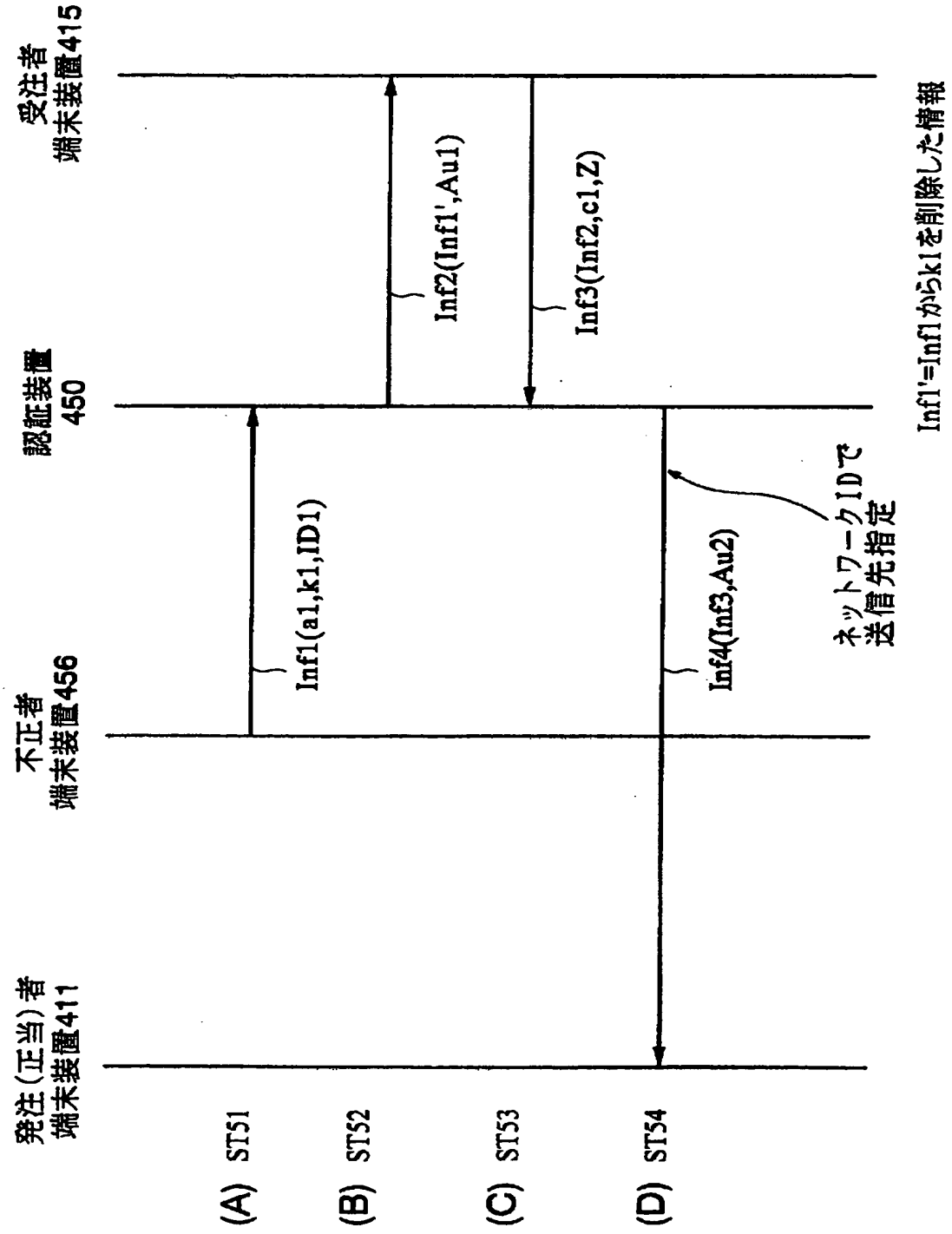
【図３７】


450 認証装置
受信部
481
送信部
482
暗号化部
483
復号部
484
記憶部
485
制御部
486
署名作成部
487
課金処理部
488

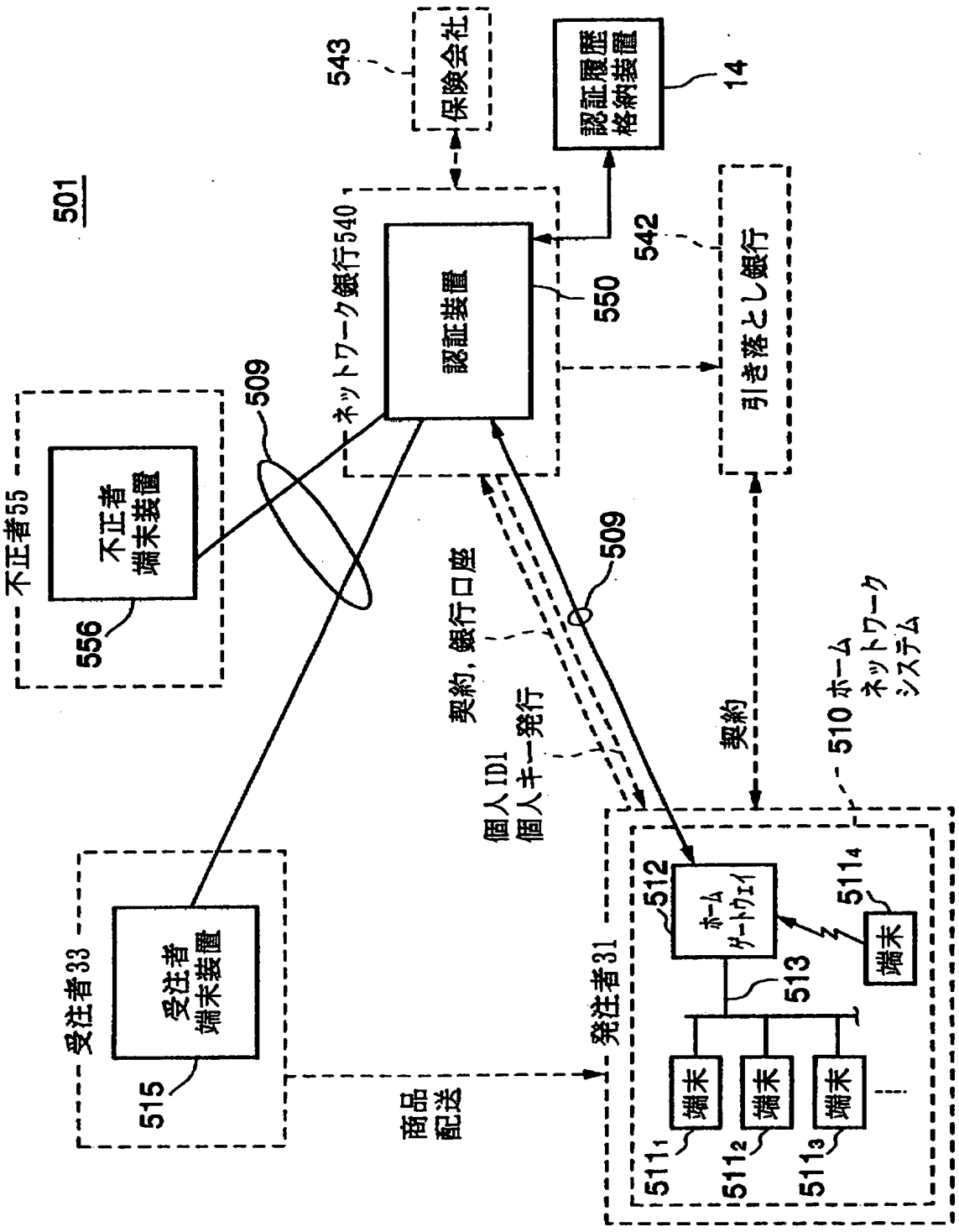
【図３８】


受注者
端末装置415
認証装置
450
発注者
端末装置411
Inf1(a1,k1,ID1)
Inf2(Inf1',Au1)
Inf3(Inf2,C1,Z)
Inf4(Inf3,Au2)
(A) ST41
(B) ST42
(C) ST43
(D) ST44
Inf1'=Inf1からk1を削除した情報

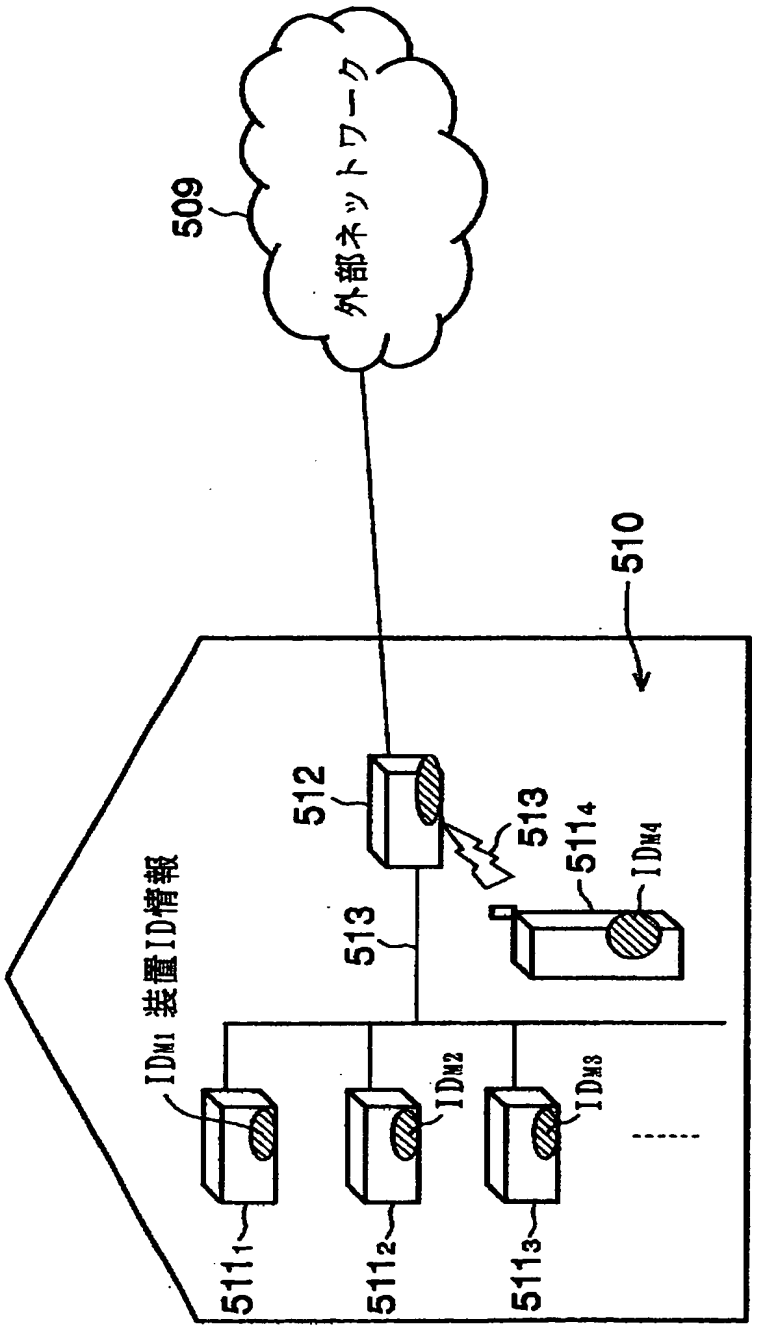
【図３９】


受注者
端末装置415
認証装置
450
不正者
端末装置456
発注(正当)者
端末装置411
Inf1(a1,k1,ID1)
Inf2(Inf1',Au1)
Inf3(Inf2,c1,Z)
Inf4(Inf3,Au2)
ネットワークIDで
送信先指定
Inf1'=Inf1からk1を削除した情報
(A) ST51
(B) ST52
(C) ST53
(D) ST54

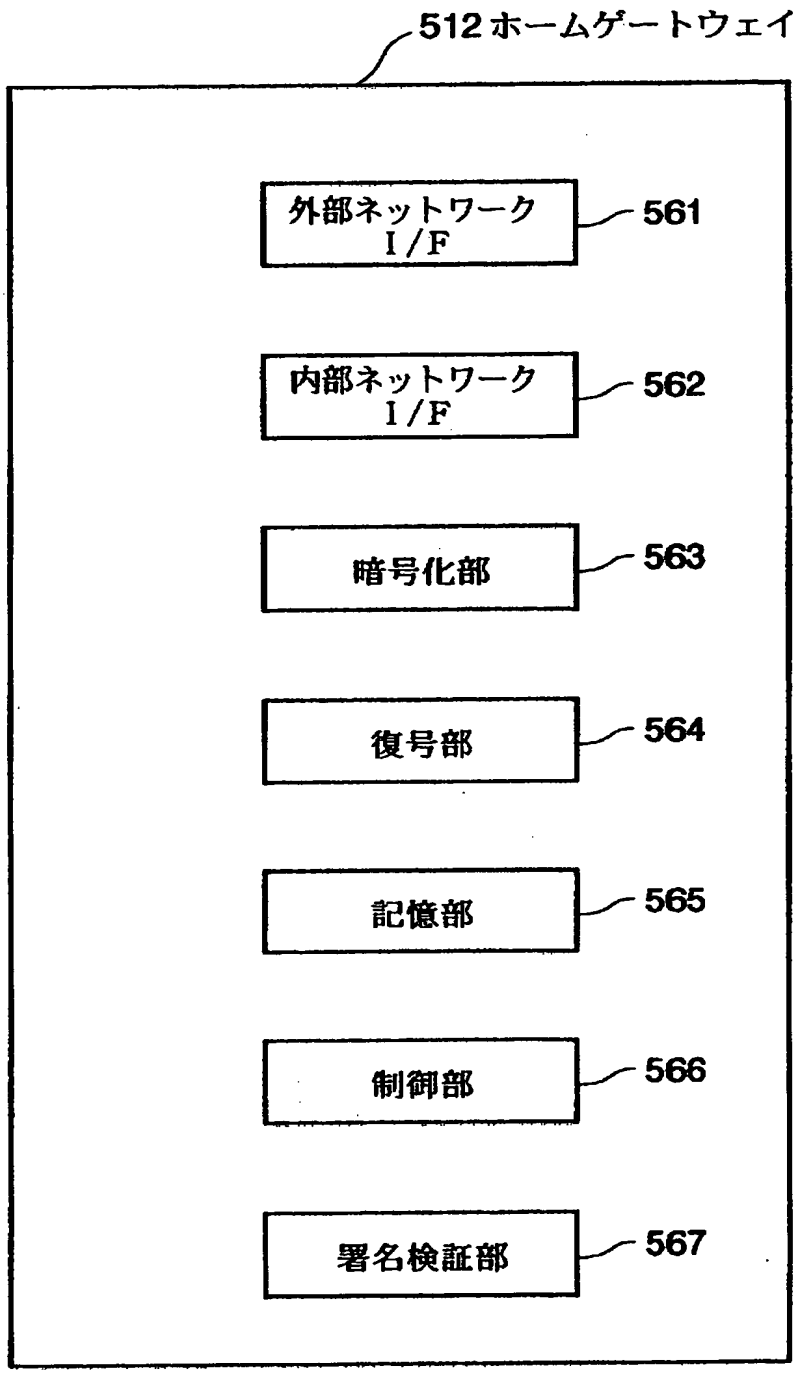
【図４０】


501
543
保険会社
認証履歴格納装置
14
ネットワーク銀行540
認証装置
550
542
引き落とし銀行
509
不正者55
不正者端末装置
556
509
契約，銀行口座
個人ID1
個人キー発行
契約
510 ホームネットワークシステム
受注者33
受注者端末装置
515
商品配送
発注者31
512
ホームゲートウェイ
513
5114
端末
5111
端末
5112
端末
5113
端末

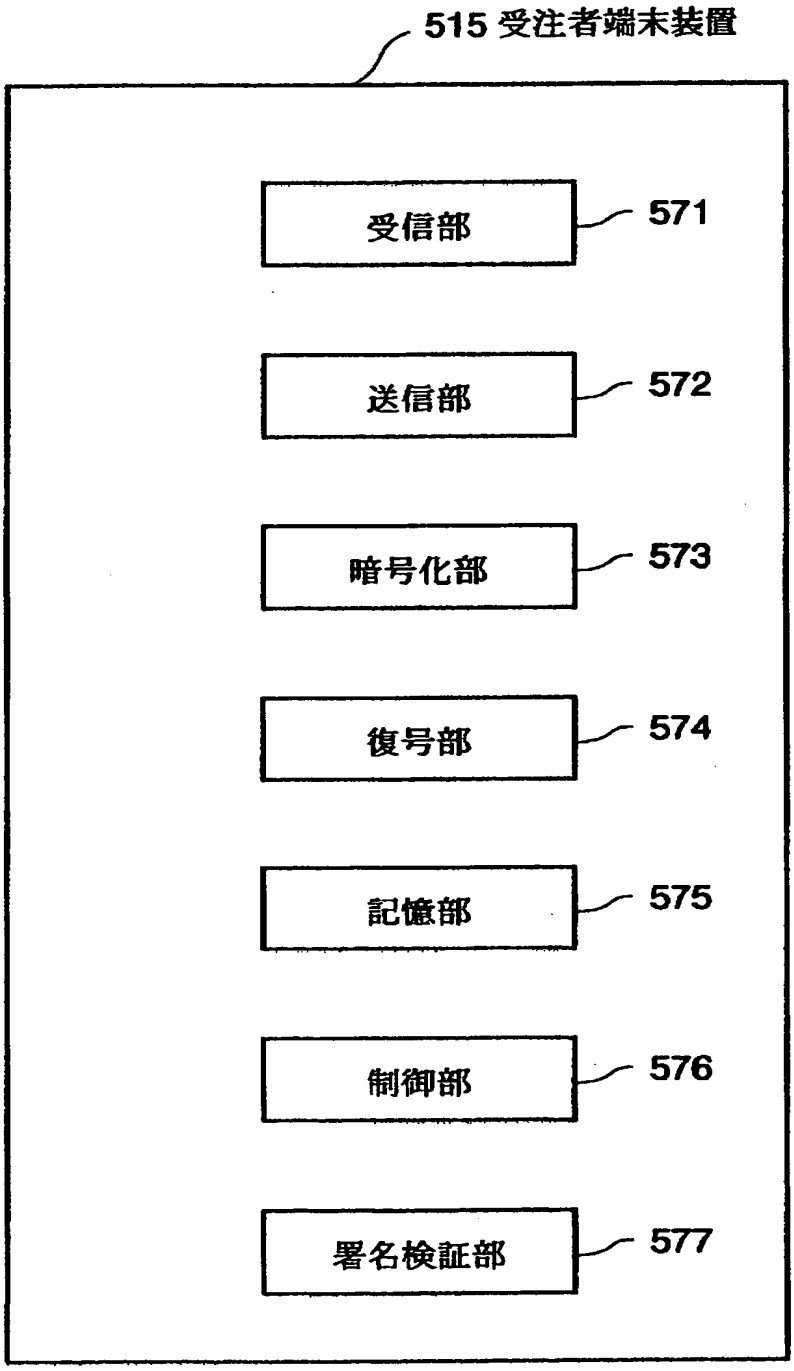
【図４１】


509
外部ネットワーク
510
512
513
513
5114
IDM4
IDM1 装置ID情報
IDM2
IDM3
5111
5112
5113

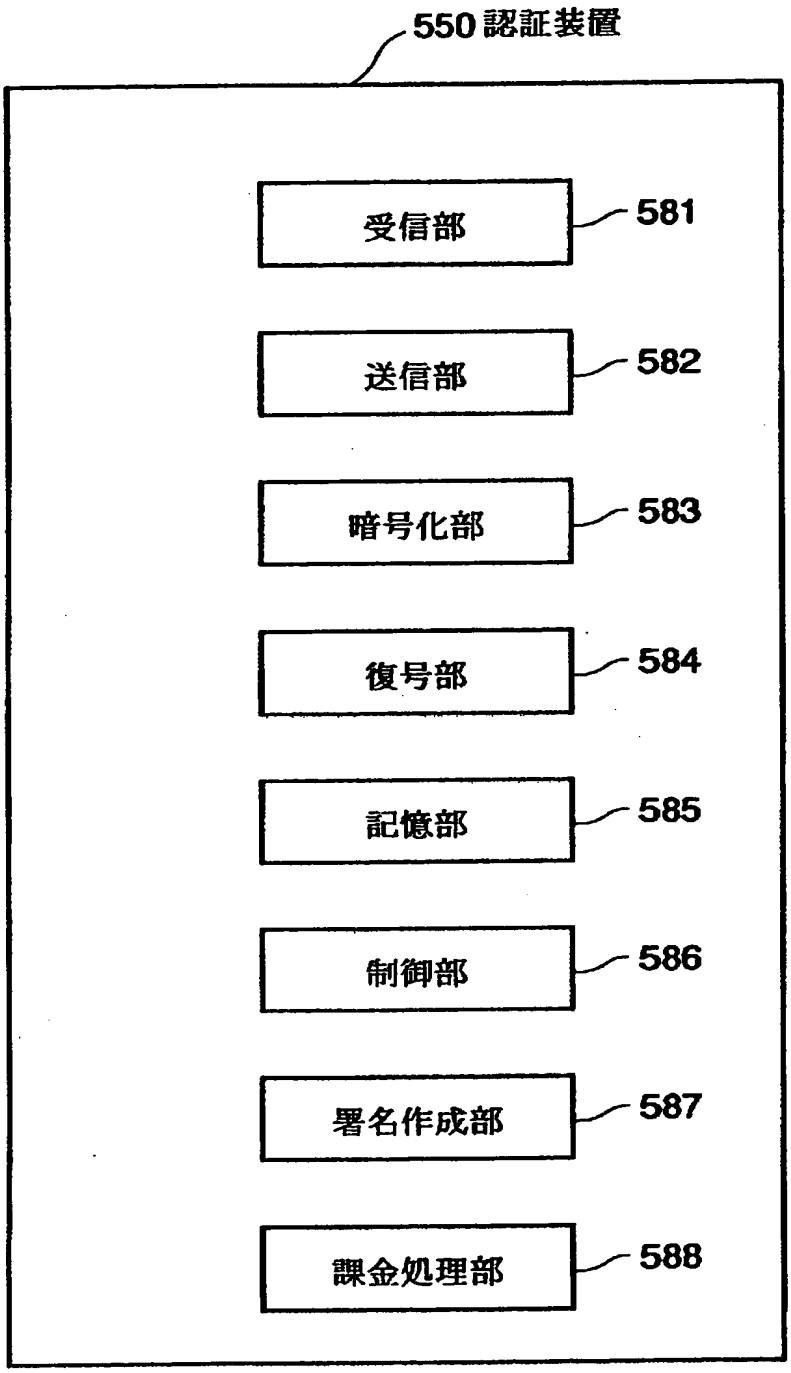
【図４２】


512 ホームゲートウェイ
外部ネットワーク I/F
561
内部ネットワーク I/F
562
暗号化部
563
復号部
564
記憶部
565
制御部
566
署名検証部
567

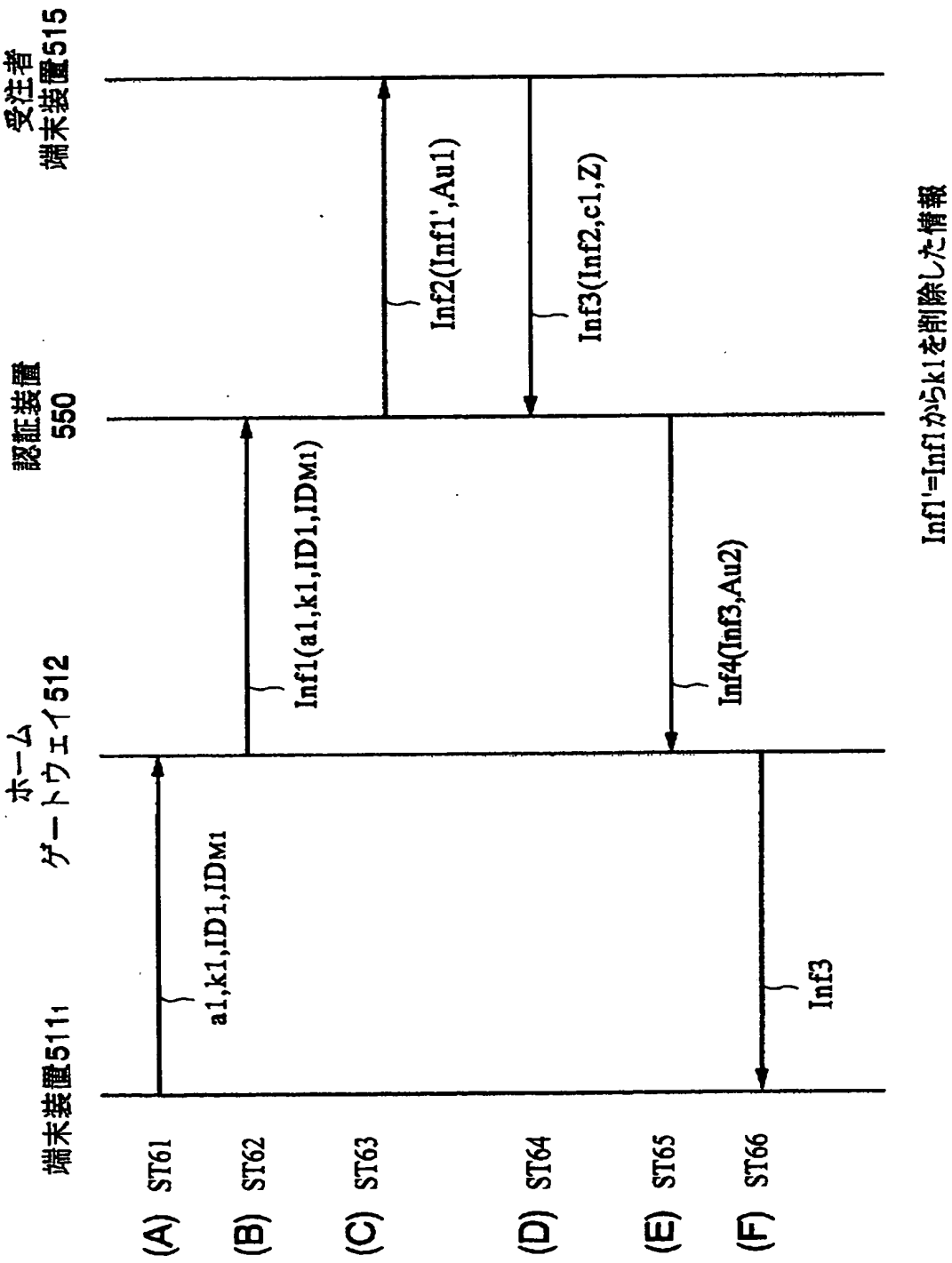
【図４３】


515 受注者端末装置
受信部
571
送信部
572
暗号化部
573
復号部
574
記憶部
575
制御部
576
署名検証部
577

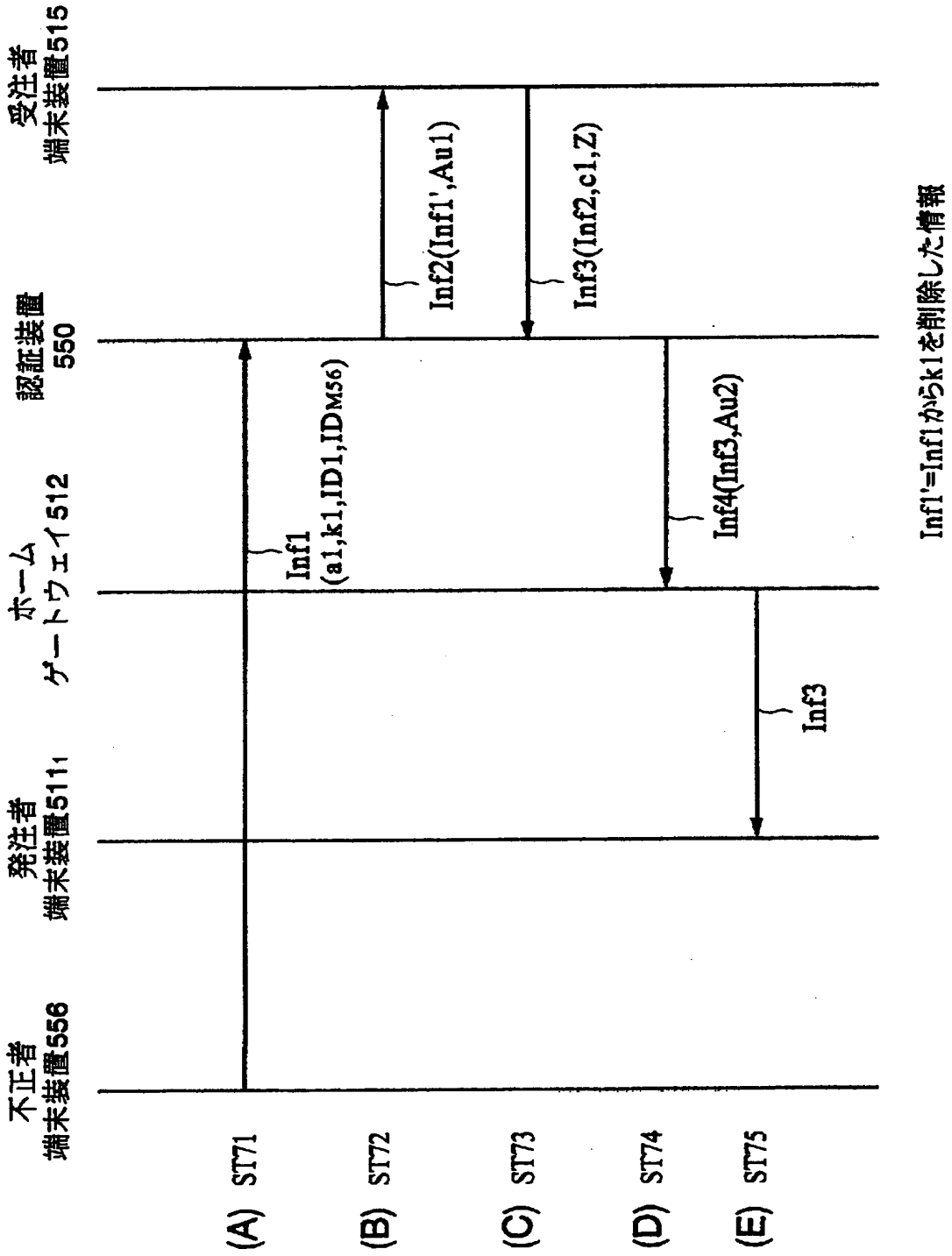
【図４４】


550 認証装置
受信部
581
送信部
582
暗号化部
583
復号部
584
記憶部
585
制御部
586
署名作成部
587
課金処理部
588

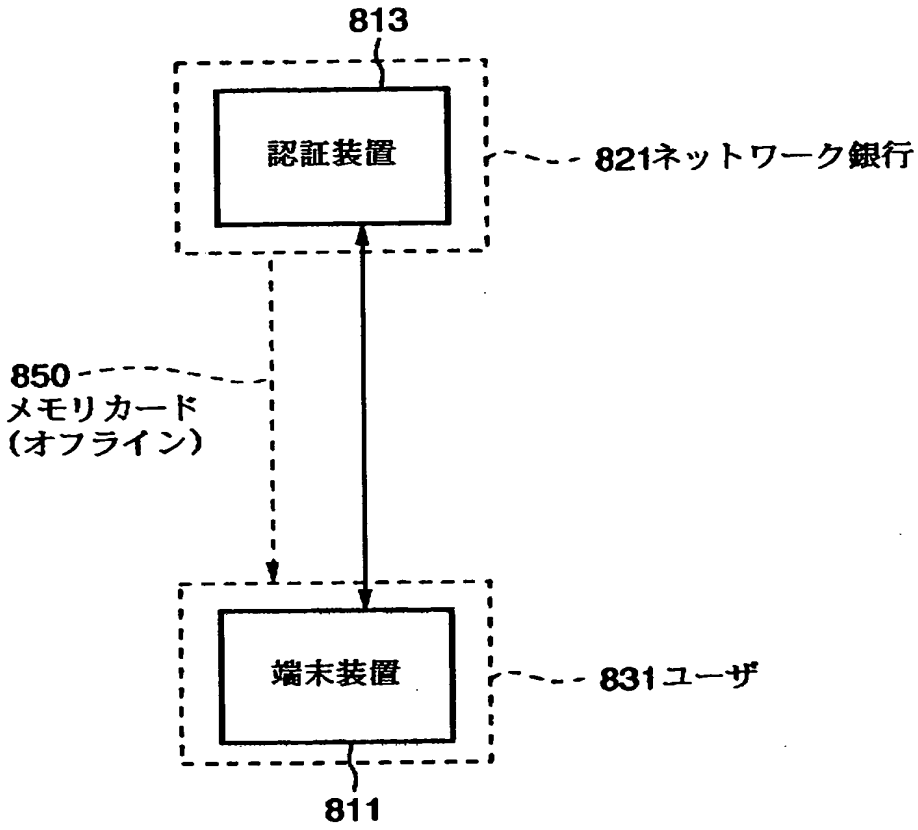
【図４５】


端末装置5111
ホームゲートウェイ512
認証装置550
受注者端末装置515
(A) ST61
(B) ST62
(C) ST63
(D) ST64
(E) ST65
(F) ST66
a1,k1,ID1,IDM1
Inf1(a1,k1,ID1,IDM1)
Inf2(Inf1',Au1)
Inf3(Inf2,c1,Z)
Inf4(Inf3,Au2)
Inf3
Inf1'=Inf1からk1を削除した情報

【図４６】

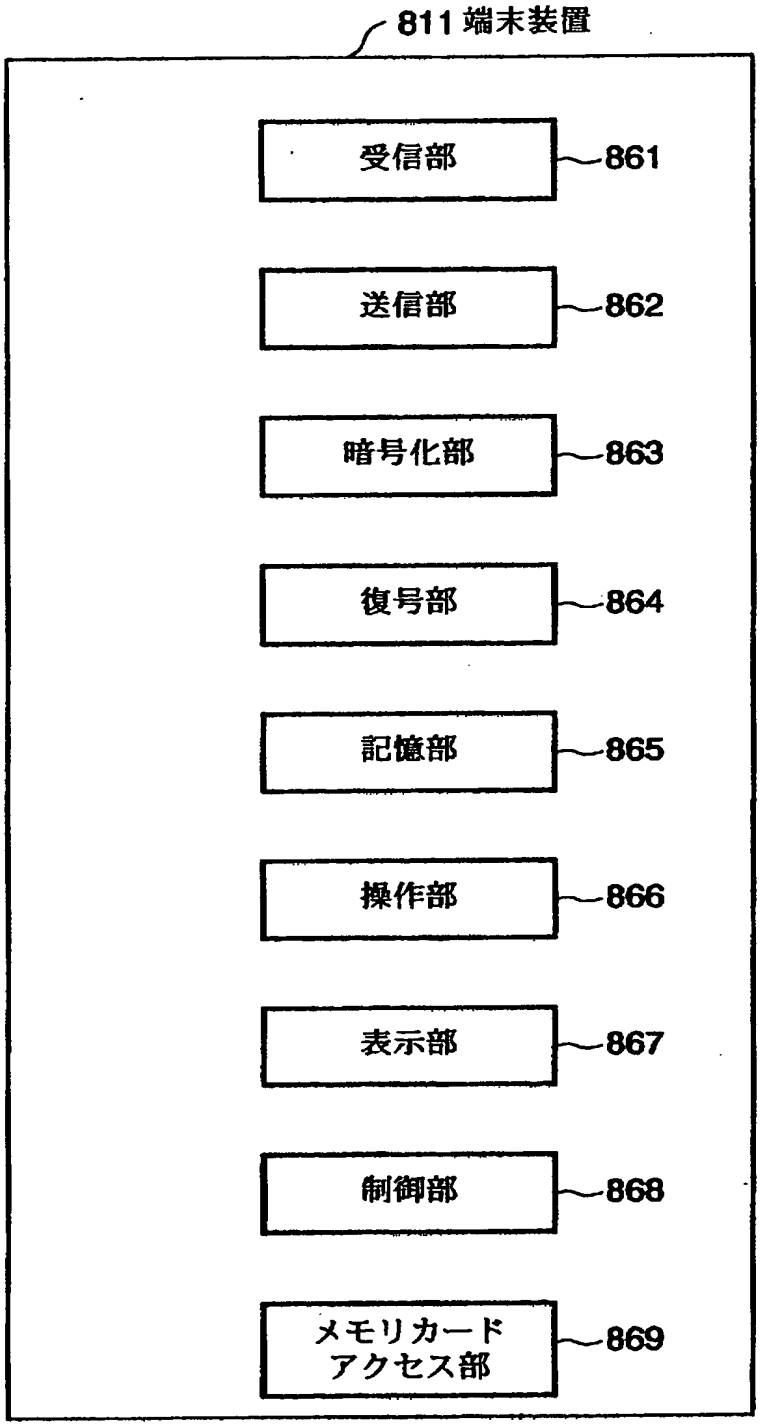

不正者
端末装置556
発注者
端末装置5111
ホーム
ゲートウェイ512
認証装置
550
受注者
端末装置515
(A) ST71
(B) ST72
(C) ST73
(D) ST74
(E) ST75
Inf1
(a1,k1,ID1,IDM56)
Inf2(Inf1',Au1)
Inf3(Inf2,c1,Z)
Inf4(Inf3,Au2)
Inf3
Inf1'=Inf1からk1を削除した情報

【図４７】

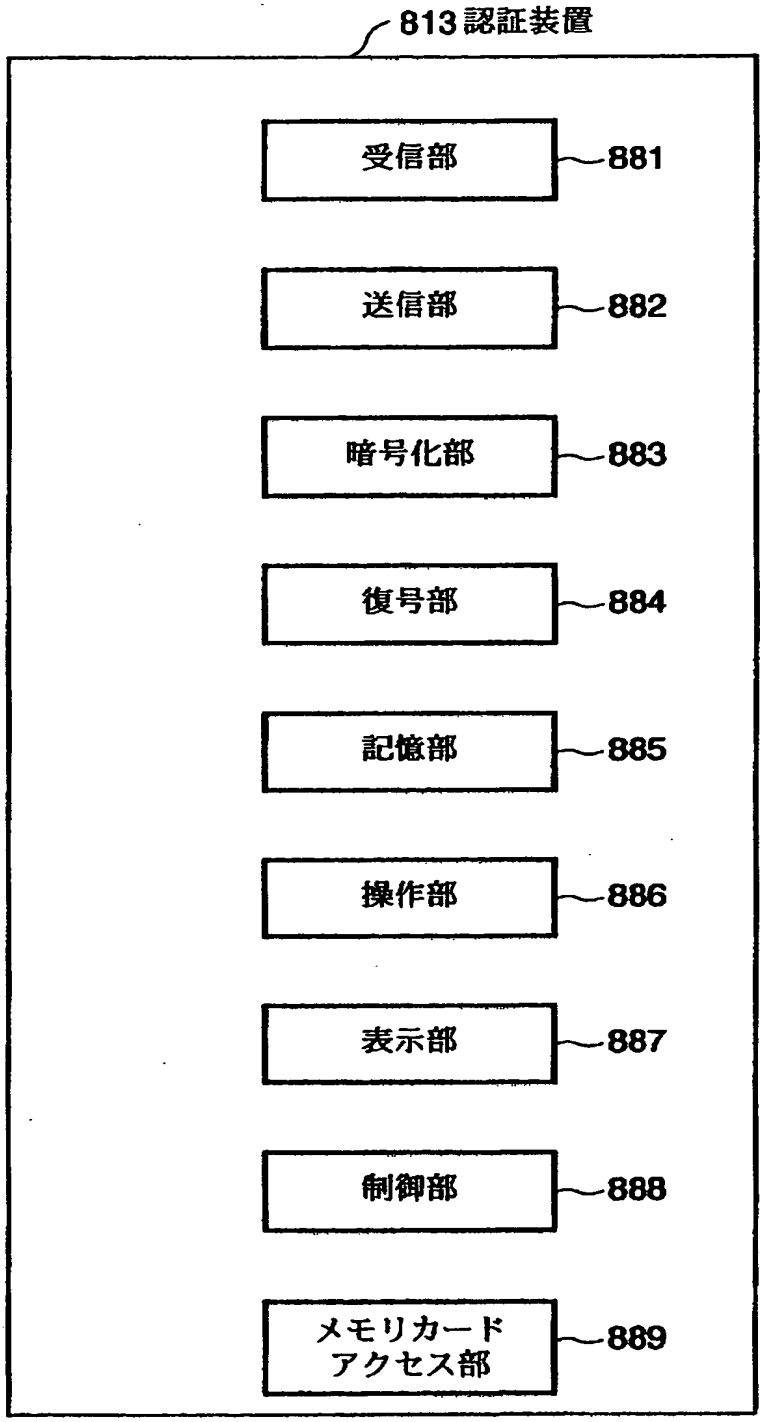


801

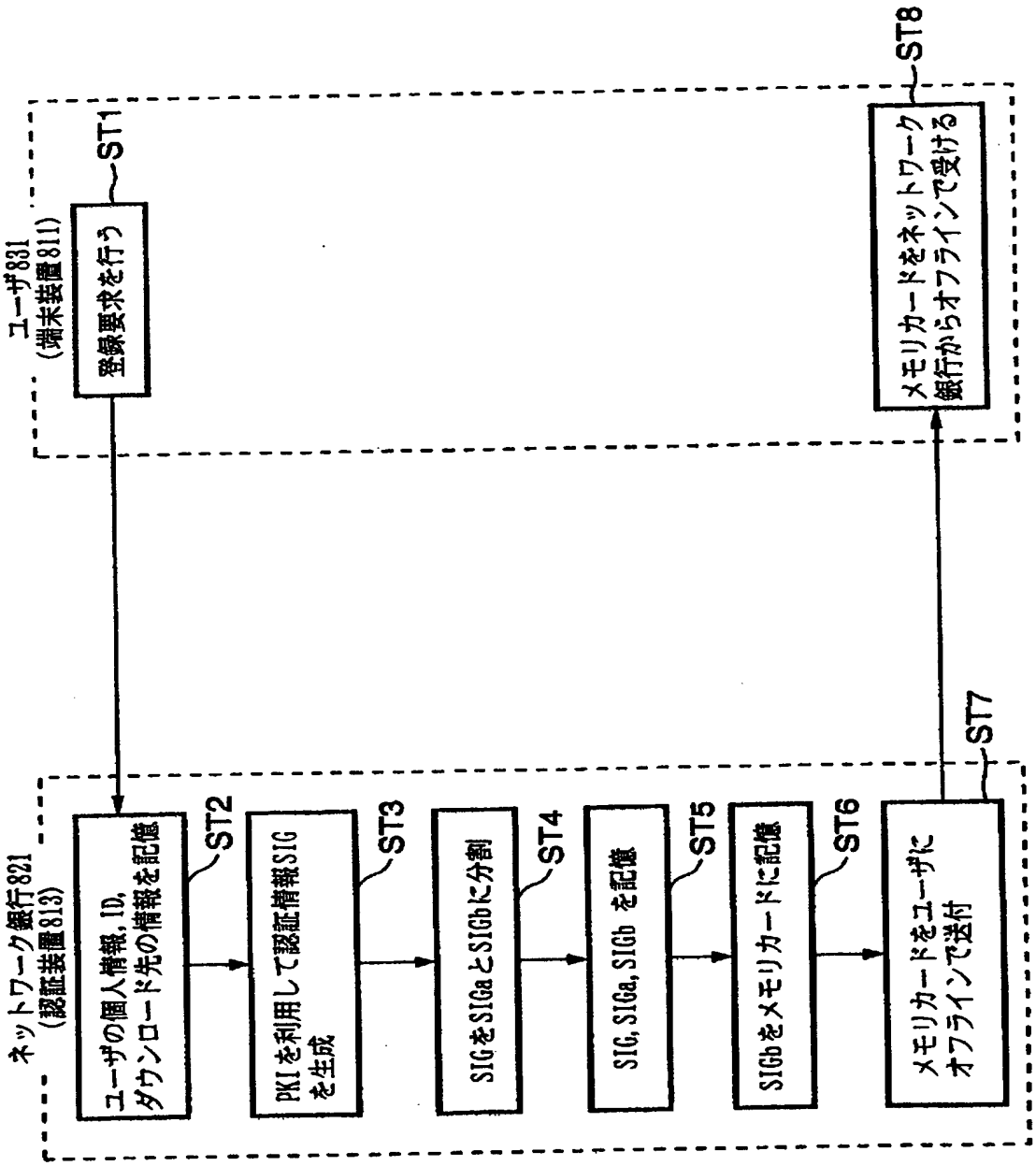
【図４８】


811 端末装置
受信部
861
送信部
862
暗号化部
863
復号部
864
記憶部
865
操作部
866
表示部
867
制御部
868
メモリカード
アクセス部
869

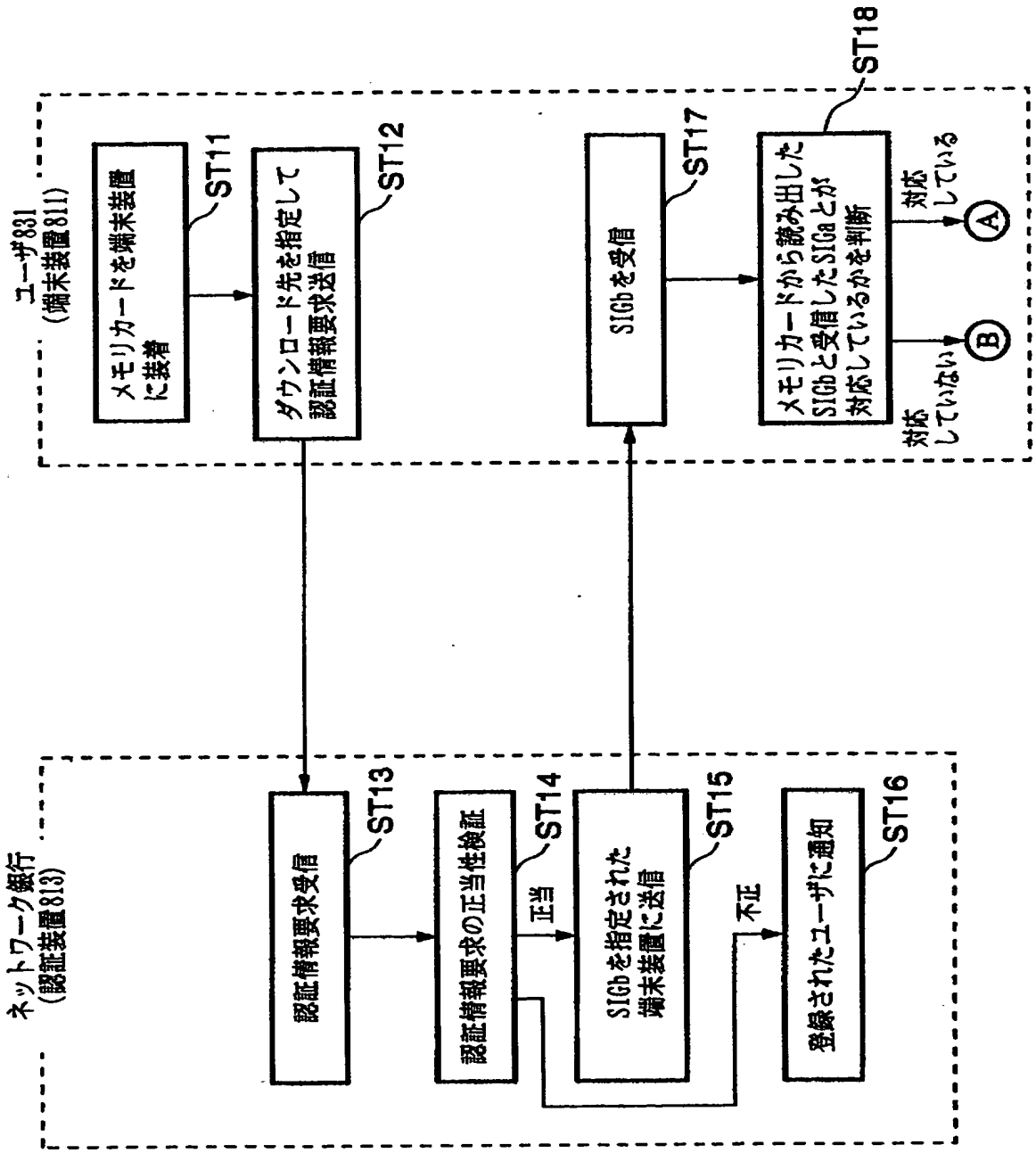
【図４９】


813認証装置
受信部
881
送信部
882
暗号化部
883
復号部
884
記憶部
885
操作部
886
表示部
887
制御部
888
メモリカード
アクセス部
889

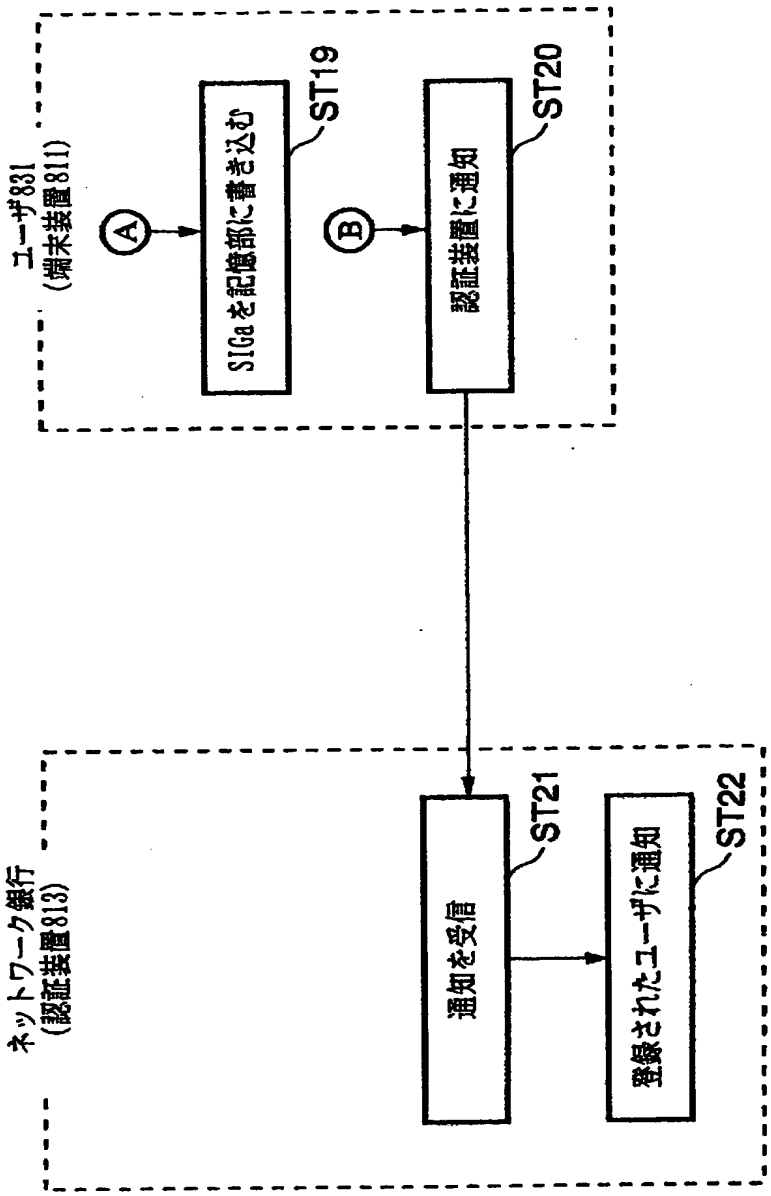
【図５０】


ユーザ831
(端末装置811)
ST1
登録要求を行う
ST8
メモリカードをネットワーク銀行からオフラインで受ける
ネットワーク銀行821
(認証装置813)
ST2
ユーザの個人情報, ID, ダウンロード先の情報を記憶
ST3
PKIを利用して認証情報SIGを生成
ST4
SIGをSIGaとSIGbに分割
ST5
SIG, SIGa, SIGb を記憶
ST6
SIGbをメモリカードに記憶
ST7
メモリカードをユーザにオフラインで送付

【図５１】


ユーザ831
(端末装置811)
メモリカードを端末装置に装着
ST11
ダウンロード先を指定して認証情報要求送信
ST12
SIGbを受信
ST17
メモリカードから読み出したSIGbと受信したSIGaとが対応しているかを判断
ST18
対応している
A
対応していない
B
ネットワーク銀行
(認証装置813)
認証情報要求受信
ST13
認証情報要求の正当性検証
ST14
正当
SIGbを指定された端末装置に送信
ST15
不正
登録されたユーザに通知
ST16

【図５２】


ユーザ831
(端末装置811)
Ⓐ
SIGaを記憶部に書き込む
ST19
Ⓑ
認証装置に通知
ST20
ネットワーク銀行
(認証装置813)
通知を受信
ST21
登録されたユーザに通知
ST22

【書類名】　　要約書

【要約】

【課題】　不正に取得した他人の個人ＩＤ情報に基づいて不正な認証手続が行われることを回避する認証装置を提供する。

【解決手段】　認証装置５０は、発注者端末装置１１からの認証要求によって、発注者３１の個人ＩＤ情報ＩＤ１と、受注者３３の個人ＩＤ情報ＩＤ２と、取り引き情報とを受信し、受注者端末装置１５との間の通信を行った後に、受注者３３の正当性を示す認証情報を発注者端末装置１１に送信する。

【選択図】　図１

認定・付加情報

特許出願の番号	特願２０００－３７９３６１
受付番号	５００００１６０９６９３
書類名	特許願
担当官	第七担当上席　　００９６
作成日	平成１２年１２月１８日

＜認定情報・付加情報＞

【特許出願人】

【識別番号】	000002185
【住所又は居所】	東京都品川区北品川６丁目７番３５号
【氏名又は名称】	ソニー株式会社

【代理人】　申請人

【識別番号】	100094053
【住所又は居所】	東京都台東区柳橋２丁目４番２号　創進国際特許事務所
【氏名又は名称】	佐藤　隆久

次頁無

出 願 人 履 歴 情 報

識別番号　〔０００００２１８５〕

１．変更年月日　１９９０年　８月３０日
［変更理由］　新規登録
住　所　東京都品川区北品川６丁目７番３５号
氏　名　ソニー株式会社